

PROTECTED A



Entry/Exit Initiative

Addendum to the Phase II Privacy Impact Assessment

Traveller Transformation Division
Policy Development Unit
March 2016



Canada

SUMMARY OF CHANGES

Purpose of the Addendum

This document has been prepared as an addendum to the Entry/Exit Phase II Privacy Impact Assessment (PIA) to notify the Office of the Privacy Commissioner of Canada (OPC) that effective June 28, 2016 (anticipated), the scope of affected travellers under the Entry/Exit Initiative will be expanded to include all foreign nationals and permanent residents crossing the shared land border between Canada and the United States (US). Specifically, information on US citizens entering either country via an automated port of entry along the land border will now be included in the scope of Entry/Exit. The personal information data elements, as well as the intended purpose for collection, will remain the same as under Phase II, as only the class of individuals will be expanded. No information on Canadian citizens and Registered Indians ("Canadians") will be exchanged with the US at this time.

The full implementation of the Entry/Exit Initiative, specifically the systematic collection of exit information on all travellers in the land and air modes, has been delayed from the initial commitment of June 2014 to provide the Government of Canada with additional time to pursue the requisite legislative authorities and to make targeted investments regarding new Information Technology (IT) systems. A new PIA will be submitted to the OPC 120 days prior to the implementation of all future deliverables of the Entry/Exit initiative.

Background

In 2011, Canada and the US issued the *Beyond the Border: A Shared Vision for Perimeter Security and Economic Competitiveness* declaration, which established a new, long-term partnership built upon a perimeter approach to security and economic competitiveness. The *Perimeter Security and Economic Competitiveness Action Plan* (Action Plan), issued later that year, sets out the joint Canada – US priorities for achieving this vision. As part of delivering on their commitments in the Action Plan, Canada and the US are undertaking the Entry/Exit Initiative.

The Entry/Exit Initiative falls under the Canada Border Services Agency's (CBSA) mandate of providing integrated border services that support national security and public safety priorities and facilitate the free flow of persons and goods, which meet all requirements under the program legislation.

The Entry/Exit Initiative will implement a system to exchange Biographic Entry Data¹ between Canada and the US, such that an entry into one country is considered an exit from the other, thereby establishing a common and integrated approach to border management. Biographic Entry Data refers to any personal information collected on foreign nationals or permanent residents that enter either Canada or the US via the shared land border which is subsequently exchanged under the Entry/Exit Initiative. This information is non-derogatory

¹ 'Biographic Entry Data' refers to any personal information collected on foreign nationals or permanent residents that enter either Canada or the US via the shared land border which is subsequently exchanged under the Entry/Exit Initiative

and consists of basic biographic data elements routinely collected from travellers entering either country, specifically: first name, last name, middle name, date of birth, nationality/citizenship, gender, travel document type, travel document number, travel document country of issuance as well as date, time, and location of entry.

The Entry/Exit Initiative will continue to be implemented through a phased approach and by making targeted investments in new technology and infrastructure, where required. Three phases of the Entry/Exit Initiative are applicable to travellers crossing the Canada - US land border, and the fourth phase involves the collection of Biographic Air Exit Data² on all travellers in the air mode. The coordinated investments in entry and exit systems will assist the Government of Canada in meeting its objective of effectively administering and enforcing Canada's immigration and border management programs. The Entry/Exit Initiative is outlined in the Action Plan and is summarized as follows:

Implemented

- **(Phase I)** September 30, 2012 – January 30, 2013: the implementation of a proof of concept to exchange the Biographic Entry Data of third-country nationals³, permanent residents of Canada and lawful permanent residents of the United States, at four automated common land border ports of entry. The proof of concept was deemed successful, thus enabling the CBSA to move on to Phase II;
- **(Phase II)** By June 30, 2013, the implementation of the Entry/Exit Initiative exchanging the Biographic Entry Data of third-country nationals, permanent residents of Canada and lawful permanent residents of the United States, at all automated land border ports of entry;

Delayed

- **(Phase III)** By June 30, 2014, the expansion of the Entry/Exit Initiative to include the exchange of Biographic Entry Data on all travellers at all automated⁴ land border ports of entry; and
- **(Phase IV)** With respect to air travel, by June 30, 2014, Canada will develop a system, under the Entry/Exit Initiative, to establish exit, similar to that in the United States.

Both countries also committed to conduct exploratory work regarding the possible future integration of entry and exit information systems in the marine and rail modes.

Current Status

Phase II of the Entry/Exit Initiative was successfully implemented on June 30, 2013. Presently, Canada and the US continue to exchange Biographic Entry Data on third-country nationals and permanent residents for

² Biographic Air Exit Data refers to any personal information collected under the Entry/Exit Initiative on all travellers departing Canada on board outbound international flights (e.g. passenger manifest information from air carriers).

³ Third country national means a person who is not a citizen of Canada or the US or a Registered Indian in Canada under each country's respective laws. Of note is that citizens of Canada and the US are out of scope for Phase II even though Canada and the US are foreign nationals to each other. The use of the term third-country nationals is meant to exclude citizens of either country.

⁴ An automated port is one that has network connectivity and access to technology, including the Integrated Primary Inspection Line (IPIL) system, to allow for the electronic capture of document information upon entry into Canada.

purposes outlined in the Phase II PIA.

Effective June 28, 2016 (anticipated), all existing activities currently in place and the uses of personal information collected and disclosed under Entry/Exit will remain the same as under Phase II, but the scope of affected individuals will be expanded under existing authorities to enable the CBSA to:

- a) Receive Biographic Entry Data from the US Customs and Border Protection (CBP) on all foreign nationals (including US citizens) and permanent residents that depart Canada and enter the US via an automated port of entry along the shared land border; and
- b) Disclose Biographic Entry Data to the US CBP for all US citizens, third-country nationals, and permanent residents that depart the US and enter Canada via an automated land border crossing.

The exchange of Biographic Entry Data on Canadians crossing the land border as well as the implementation of an air exit system to collect Biographic Air Exit Data on all travellers leaving Canada on board international flights will be deferred until the requisite legislative and regulatory amendments are in place (currently anticipated for Fall 2017).

Biographic Entry Data collected under Phase II of the Entry/Exit Initiative is not currently being disclosed to other federal government departments systematically. As noted in the Phase II PIA, this information may only be disclosed on an *ad hoc* basis subject to specific legislative authorities that govern the disclosure and collection of this information. All *ad hoc* requests for Biographic Entry Data received by the CBSA will continue to be processed on a case-by-case basis.

Systematic disclosures to other government departments are currently under consideration for future phases. The additional privacy compliance analysis for these disclosures will be clearly outlined in a subsequent PIA that will be submitted to the OPC 120 days prior any new disclosures occurring.

As outlined in the Phase II PIA, exchanged Biographic Entry Data will continue to be used under the current phase to effectively administer and enforce the immigration laws of Canada, by:

1. Reconciling Biographic Entry Data received from the US to traveller records previously collected by the CBSA;
2. Facilitating the CBSA's ability to focus immigration enforcement actions and investigations on warrants for foreign nationals and permanent residents who are suspected to still be in Canada;
3. Facilitating the CBSA's ability to focus immigration enforcement actions and investigations on foreign nationals subject to removal orders who are suspected to still be in Canada;
4. Facilitating the CBSA's ability to determine the whereabouts of foreign nationals and permanent residents for the purpose of admissibility determination to Canada, including those

who may be a threat to Canada's national security; and

5. Possibly identify program integrity issues.

Process, data exchange and timeframe:

The process for exchanging data is the same as outlined in the Phase II PIA.

The increased collection and disclosure of information is forecasted to start at 12:01am on June 28, 2016 (anticipated). After this date, the information will be exchanged between Canada and the US in near real-time.

Legal authorities for the collection, use and disclosure of Biographic Entry Data on foreign nationals and permanent residents:

- *Canada Border Services Agency Act*, subsection 5(1)
- *Immigration and Refugee Protection Act*, subsection 4(2), paragraph 20(1)(b), and subsection 28(1)
- *Privacy Act*, sections 4, 7 and subsection 8(2)

UPDATE ON KEY PRIVACY RECOMMENDATIONS

Memorandum of Understanding with the US:

The Phase II PIA identified a “moderate” risk of possible onward disclosure of Entry/Exit information due to existing requirements within US law. The *Annex Regarding the Sharing of Biographic Entry Data to the 2003 Statement of Mutual Understanding on Information Sharing* (the Annex) between the CBSA, Immigration, Refugees and Citizenship Canada (formerly known as Citizenship and Immigration Canada) and the Department of Homeland Security (DHS) has been established to mitigate this risk by establishing a framework to limit the purposes of the exchange to national security related cases. Specifically, the Annex outlines that information sharing must be done in accordance with the Beyond the Border Action Plan: Statement of Privacy Principles, including all authorized secondary uses and onward disclosures, and ensures that there are mechanisms in place to address any potential violation to the agreement. The purpose and scope of the Annex is limited to Third Country Nationals and Permanent Residents, and does not address information sharing on US citizens.

Notice

The CBSA will post new temporary signage (as was done previously to support the implementation of Phase II) at all implicated land border crossings to notify affected travellers, including US citizens, that their personal information is being collected and exchanged with the US under the Entry/Exit Initiative.

As a result, the CBSA will ensure that signs posted at Canadian POEs will include language to notify affected travellers that the CBSA collects their personal information from the CBP when they enter the US by land, so that a record of entry into one country can serve as the record of exit from the other.

All future signs will also include provisions to direct individuals to the CBSA website should they require additional information on the Entry/Exit Initiative, including the Entry/Exit Traveller Processing Personal Information Bank (PIB).

The CBSA will also continue to employ a variety of communication vehicles to notify affected travellers and the general public of the collection, use, disclosure and protections surrounding information gathered through the Entry/Exit Initiative.

Retention Period

In an effort to be consistent with other existing immigration programs (i.e. uses of personal information for non-citizens), an initial retention period of 75 years was established for Phase II of the Entry/Exit Initiative. The CBSA has since conducted a thorough analysis of the proposed future uses, and the retention period will be significantly reduced from 75 to 15 years effective June 28, 2016. Biographic Entry Data collected under Entry/Exit will be kept for a period of 15 years, and will then be purged from CBSA data holdings, unless they are required to support active and ongoing CBSA immigration enforcement investigations or it has been less than two years since the information was used to support an administrative decision.

The proposed retention period of 15 years is necessary to support lengthy immigration enforcement investigations conducted in accordance with the Agency's mandate and to enhance border management by providing the CBSA with reliable and accurate travel history information to support improved domain awareness regarding foreign nationals and permanent residents crossing Canada's border.

The reduced retention period will apply retroactively to all Biographic Entry Data already collected under Phase II of the Entry/Exit Initiative, as well as to any Biographic Entry Data and Biographic Air Exit Data collected under future phases. The Entry/Exit Traveller Processing PIB has been updated accordingly and will be published on Info Source by June 28, 2016 to notify the general public about the reduced retention period.

All uses of Biographic Entry Data collected under Entry/Exit after June 28, 2016 will remain the same as outlined under the Phase II PIA, until the program is further expanded under future phases to include Canadians once the required legislative and regulatory authorities are in place. The CBSA commits to submit a separate PIA to the OPC to outline the use, management, disclosure, and protection of personal information for all future phases of the Entry/Exit Initiative, including the collection of personal information on all travellers in the air mode, as well as on Canadians in the land mode.

UPDATE TO THE PERSONAL INFORMATION BANK

Description of the class of records associated with the program or activity:

Traveller Processing

Description: Describes records related to people, goods and conveyances arriving at Canadian ports of entry and records of individuals departing Canada. May include records related to the establishment or use of electronic systems used to administer or manage the program including the Integrated Customs Enforcement System (ICES), Integrated Primary Inspection Line (IPIL), Passenger Information System (PAXIS), Telephone Reporting Centre System (TRCS), Secondary Processing System, Passage History Database, Occurrence Reporting System (ORS), Intelligence Management System (IMS), Integrated Border Query (IBQ), Field Operations Support System (FOSS), Computer Assisted Immigration Processing System (CAIPS), Canadian Police Information Centre (CPIC), National Crime Information Center (NCIC), Client Status Query (CSQ), Modern War Crimes System (MWCS), Secure Tracking System (STS), Support System for Intelligence (SSI), National Case Management System (NCMS), Global Case Management System (GCMS), Automated Fingerprint System (AFIS).

Document Types: Forms, manuals, policy, memoranda of understanding, passage and enforcement history.

Class of Record Number:

CBSA ENF 129

- ☐ Proposal for a New Personal Information Bank
- ☒ Proposal to modify an existing Personal Information Bank - identify PIB registration number and current description:

Entry / Exit Traveller Processing Personal Information Bank

Description: This bank describes information about individuals who enter Canada through all modes of travel or leave Canada through automated common land border crossings between Canada and the United States (US). The personal information collected may include, and are limited to, traveller entry and exit data elements as follows: first/given name(s), middle name(s), last name/surname(s), nationality (citizenship), date of birth, gender, travel document type (e.g., passport), travel document number, travel document country of issuance, port of entry, date and time of entry. For individuals entering Canada from the US, this information is collected as an extraction of the personal information currently collected as part of the CBSA's traveller processing activities. For individuals exiting Canada across the shared Canada US border, this information is collected by US Customs and Border Protection officials upon entry into the US and subsequently shared with Canada pursuant to an information sharing agreement between Canada and the US. Under the auspices of the *Beyond the Border Action Plan: A Shared Vision for Perimeter Security and Economic Competitiveness*, Canada and the US share biographic entry data such that an entry into one country is considered an exit from the other thereby establishing an integrated and coordinated approach to border management.

Class of Individuals: Foreign nationals, permanent residents of Canada and lawful permanent residents of the United States.

Purpose: The personal information is collected and used for the purposes of improving border management by enabling the CBSA to monitor the flow of persons entering and departing from Canada. In effect, this will enhance the public safety and security of Canada by increasing the effectiveness of the Admissibility Determination and Immigration Enforcement program activities by enabling these functions to better determine who has left Canada. Personal information is collected pursuant to the *Canada Border Services Agency Act* subsection 5(1), the *Immigration and Refugee Protection Act (IRPA)* subsection 4(2), paragraph 20(1)(b) and subsection 28(1).

Consistent Uses: The information may be used or disclosed internally for the following purposes: statistical analysis, program administration and program evaluation. The data collected regarding the class of individuals listed will be compared against extracts of immigration warrants, removal orders, and a subset of Enforcement Information Index lookouts to: facilitate the CBSA's ability to focus immigration enforcement actions and investigations on persons in Canada; and facilitate the Government of Canada's ability to determine the whereabouts of persons whom are wanted for reasons of national security, serious criminality, crimes against humanity or war crimes, and organized criminality. Please refer to *Enforcement Information Index System (EIIIS) CBSA PPU 025* and *Immigration Warrant File CBSA PPU 026*. The data collected in this bank will be reconciled against a non-operational copy of information stored in the *Traveller Processing Personal Information Bank CBSA PPU 1101* to create a record of departures from Canada and to enable the accumulation of traveller history information. Statistical analyses of the data will be conducted to: evaluate program integrity and gain insight into trends and patterns to inform program policy decisions. Information may also be disclosed to the United States of America Customs and Border Protection for the purposes of administering and enforcing US immigration laws and in support of activities related to law enforcement and national security. Disclosure of the information to the US is completed pursuant to the *Beyond the Border Action Plan: A Shared Vision for Perimeter Security and Economic Competitiveness*. Information may also be disclosed on an *ad hoc* basis to *Immigration, Refugees and Citizenship Canada (IRCC)*; refer to: *Immigration Case File IRCC PPU 042*, *Royal Canadian Mounted Police (RCMP)*; refer to: *Criminal Operational Intelligence Records RCMP PPU 015* and *Canadian Security Intelligence Service (CSIS)*; refer to: *Canadian Security Intelligence Service Investigational Records CSIS PPU 045* for the purposes related to immigration administration and enforcement, law enforcement, or national security.

Retention and Disposal Standards: Personal information collected under this initiative is stored in the Entry Exit Information System (EXIS). Personalised records will be retained for 15 years and will then be destroyed unless they are required to support active and ongoing CBSA immigration enforcement investigations or it has been less than two years since the information was used to support an administrative decision.

RDA Number: 2006/004

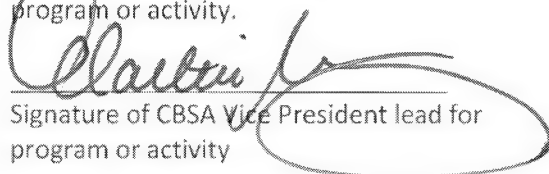
Related Record Number: CBSA ENF 129

TBS Registration: 20120435

Bank Number: CBSA PPU 1202

FORMAL APPROVAL

The following signature represents a commitment to comply with sections 4 to 8 of the *Privacy Act* and the related privacy policy requirements outlined in the CBSA PIA as they relate to the administration of the identified program or activity.


 Signature of CBSA Vice President lead for program or activity

18/03/2016
 Date

Note: Responsibility for sections 4 to 8 of the *Privacy Act* rests with all employees of government institutions that handle personal information. Officials who manage such programs and activities are responsible for ensuring that such requirements are implemented as part of the administration of the program or activity.

The following signature represents a commitment by the Head of the institution or his/her delegate(s) who is responsible for establishing personal information banks in accordance with section 10 of the *Privacy Act*.

 FOR DAV PROULX
 Signature of CBSA ATI and Privacy Director

23/03/2016
 Date

Note: Under the *Privacy Act*, the Head or his/her delegate(s) is responsible for complying with legal and relevant privacy policy requirements related to the approval and registration of personal information banks

ANNEX A: UPDATE TO PHASE II PIA ACTION PLAN

This table summarizes the privacy risks identified through the PIA process, and categorizes risk levels as low, moderate or high. Risks are expressed in terms of both likelihood of the risk occurring and the impact should it occur. The goal of privacy risk management is to identify and maintain privacy risks within acceptable bounds. The higher ratings provide an indication of priority areas for implementing suggested risk mitigation mechanisms or strategies. Although a number of mitigation strategies are discussed, some are posed as alternatives, and the implementation of all strategies is not necessarily required to address the specified privacy risks. The Elements listed below correspond with the "Canadian Standards Association Model Code for the Protection of Personal Information" (10 Fairness Principles) and the Beyond the Border Action Plan: Statement of Privacy Principles by the United States and *Canada*.

Criteria for ranking are set as follows:

- **Low:** There is a remote possibility that the risk will materialize and/or the impact of the risk to the program is minor.
- **Moderate:** The possibility of the risk materializing is very low although the impact of such a risk is high, *OR* the possibility of the risk materializing is high but the impact of such a risk is minor, *OR* the impact and likelihood of the risk occurring are both determined to be moderate.
- **High:** There is a near certainty that the risk will materialize if no corrective measures are taken and/or the impact of the risk on the program is severe.

Action Plan

Element	Nature of risk	Level of risk			Mitigating Mechanisms
		Low	Moderate	High	
Onward Disclosure (US Citizens)					At all times, the disclosure of all personal information exchanged under the Entry/Exit Initiative will be protected through existing privacy guidelines outlined in the <i>Beyond the Border Action Plan: Statement of Privacy Principles by the United States and Canada</i> and will be governed by Canada and US privacy laws.



Canada Border Services Agency— Criminal Intelligence Service Canada Information Sharing Framework Privacy Impact Assessment (PIA)

Enforcement and Intelligence Operations Directorate
Operations Branch
Canada Border Services Agency
January 2017 / Ver. 0.9



Canada

Change Control Table

Version	Date	Change Made By	Change Requested By	Change
1	Oct 29, 2016	R. Gilbert		First draft
2	Jan 13, 2016	R. Gilbert	Program	Added provincial bureaus
3	Jan 25, 2016	R. Gilbert	W. Kitto, C. Desmarais	Various edits
4	Jul 18, 2016	N. Koutros	CISC	Edits to reflect input from CISC
5	Aug 11, 2016	A.Chaudhari	N. Koutros	Various edits
6	Aug 13, 2016	N.Koutros	Internal Stakeholders	Additions following consultation w/IBD
7	Oct 12, 2016		RCMP	Modifications following external stakeholder consultation
8	Dec 2, 2016	A.Cruickshank	Internal Stakeholders	Various edits
9	Jan 25, 2017	A.Cruickshank	RCMP	Removal of NTC and analytical products

Table of Contents

CHANGE CONTROL TABLE.....	2
EXECUTIVE SUMMARY	5
ABBREVIATIONS AND ACRONYMS.....	8
DEFINITIONS.....	9
SECTION 1 - OVERVIEW AND INITIATION	11
SECTION 2 - RISK AREA IDENTIFICATION AND CATEGORIZATION	22
2.1 Type of Initiative	22
2.2 Type of Personal Information Involved and Context.....	22
2.3 Initiative Partners and Private Sector Involvement.....	23
2.4 Duration of the Initiative	23
2.5 Program Population	23
2.6 Technology and Privacy	24
2.7 Personal Information Transmission.....	24
2.8 Risk to CBSA from a Breach (Court Data).....	25
2.9 Risk to Individual from a Breach (Court Data)	25
2.10 Risk to CBSA from a Breach (ACIIS Data)	26
2.11 Risk to Individual from a Breach (ACIIS Data).....	26
SECTION 3 - ANALYSIS OF PERSONAL INFORMATION ELEMENTS	27
SECTION 4 - FLOW OF PERSONAL INFORMATION	40
SECTION 5 - PRIVACY COMPLIANCE ANALYSIS	54
5.1 Legal Authority for Collection of Personal Information.....	54
5.2 Necessity to Collect Personal Information	54
5.3 Authority for the Collection, Use or Disclosure of the Social Insurance Number ..	54
5.4 Direct Collection - Notification and Consent (as appropriate)	55
5.5 Indirect Collection - Consent or Authority under Sec. 10 of Privacy Regulations ..	55
5.6 Indirect Collection - Without Notification and Consent	55
5.7 Retention and Disposal of Personal Information	56
5.8 Accuracy of Personal Information	56
5.9 Use of Personal Information	57
5.10 Disclosures Directly Related to the Administration of the Initiative.....	58
5.11 Accounting For New Uses or Disclosures Not Reported in CBSA Info Source	60
5.12 Safeguards - Statement of Sensitivity	61
5.13 Safeguards - Threat and Risk Assessment	61
5.14 Safeguards - Administrative, Physical and Technical	61
5.15 Technology and Privacy - Tracking Technologies	63
5.16 Technology and Privacy - Surveillance or Monitoring.....	63
5.17 Considerations Related to Compliance, Regulatory Investigation, Enforcement	63
SECTION 6 – SUMMARY OF ANALYSIS AND RECOMMENDATIONS.....	65
SECTION 7 - SUPPLEMENTARY DOCUMENTS LIST	67
SECTION 8 - FORMAL APPROVAL	68
ANNEX A: PRIVACY COMPLIANCE CHECKLIST AND OTHER CONSIDERATIONS.....	69

ANNEX B: OFFICE OF THE PRIVACY COMMISSIONER EXPECTATIONS	72
ANNEX C: PIA ACTION PLAN.....	75
ANNEX D: CBSA GOVERNANCE MODEL – ACCESS AND USE OF THE AUTOMATED CRIMINAL INTELLIGENCE INFORMATION SYSTEM.....	77
ANNEX E – CBSA – CISC STATEMENT OF COOPERATION.....	87
ANNEX F – RESOLUTION CISC 2014-04 CISC-CBSA INCREASED INFORMATION SHARING.....	91
ANNEX G – CBSA-CISC MEMORANDUM OF UNDERSTANDING.....	93

Privacy Impact Assessment Date / Version:	January 2017
Office of the Privacy Commissioner file #:	
Project Implementation Plan (if applicable)	
Federal Institution:	Canada Border Services Agency (CBSA)
Related Class of Record Number:	CBSA ENF 1401 – Intelligence Program CBSA ENF 123 – Criminal Investigations Program CBSA ENF 130 – Immigration Investigation Program
Personal Information Bank:	CBSA PPU 035 – Intelligence Program CBSA PPU 1402 – Criminal Investigations Program CBSA PPU 1403 – Immigration Investigations Program
Government Official Responsible for PIA:	Vice President, Operations Branch
Delegate for section 10 of the <i>Privacy Act</i> :	ATI and Privacy Director

EXECUTIVE SUMMARY

The purpose of this PIA is to identify potential privacy risks related to the collection, use and disclosure of personal information shared between the Canada Border Services Agency (CBSA) and the Criminal Intelligence Service of Canada (CISC) and the recommended strategies to mitigate potential privacy risks related to the collection, use and disclosure of personal information among partner agencies.

Established in 1970, CISC's membership is comprised of nearly 400 law enforcement agencies and is administered under the stewardship of the Royal Canadian Mounted Police (RCMP). CISC's fundamental purpose is to facilitate the timely production and exchange of criminal intelligence information to the law enforcement community at the municipal, provincial, and federal levels. A limited number of investigators in police agencies use the information stored in ACIIS to support the detection, prevention, and disruption of serious and organized crime in Canada.

The CBSA will disclose publically available court records related to customs and immigration offences into CISC's Automated Criminal Intelligence Information System (ACIIS) when there are reasonable grounds to believe the offence has a nexus to serious or organized crime. Partners will search this information using the Intelligence Information System (IIS) query tool to support a specific lawful investigation. Partners may also request additional information related to the publically available court records through the standard written request process currently outlined in the CBSA *Policy on the Disclosure of Personal Information: Section 8 of the Privacy Act* for immigration information and in the *Policy on the Disclosure of Customs Information: Section 107 of the Customs Act* for customs information.

The CBSA's investigative bodies will collect personal information uploaded into ACIIS by law enforcement agencies to support ongoing lawful investigations of customs and immigration-related offences with a nexus to serious and organized crime. Offences investigated under the *Customs Act* include secreting illicit goods in an attempt to smuggle controlled goods, such as weapons or narcotics,

across the Canadian border (section 159). Offences investigated under the *Immigration and Refugee Protection Act* (IRPA) includes, but is not limited to, serious criminality (section 36) and for involvement in organized crime (section 37) which may cause an individual to be inadmissible to Canada. In all circumstances where queries to the ACIIS yield a match, the CBSA must make a written request detailing the specific information the CBSA is seeking, the authority to request and use that information, and the offence the information will be used to investigate. In addition, the CBSA must limit the use of this information to the investigation of serious and organized crime and agree to abide by any restrictions imposed by the originating body, in accordance with s. 7(b) of the *Privacy Act* and the supporting *CBSA Governance Model*.

The scope of this PIA is focused on the disclosure of publically available court records by the CBSA, the collection and use of personal information by the CBSA from the ACIIS using the Intelligence Information System (IIS) query tool, and the collection of additional data via a written request to the originating agency.

ACIIS is Canada's primary law enforcement database for organized crime. It contains sensitive financial, biometric, and biographic personal information as well as detailed descriptions related to suspects' criminal history, associations, and other sensitive personal information. The National Executive Committee (NEC) of the CISC will provide direct access to ACIIS unrestricted data to select members of the four CBSA investigative bodies (Inland Enforcement Division, Intelligence Operations and Analysis Division, Criminal Investigations Division, and National Security Screening Division). As a Category II(a) member, the CBSA will be granted access to ACIIS, based on the Agency's responsibilities and legislative mandate to support lawful investigations of serious and organized crime, but must submit a written request to the originating agency prior to any use of information collected from ACIIS. The CBSA intends to sign an MOU with CISC to further define each partner's responsibilities (see Annex G); however, personal information will be shared between the CBSA and provincial partners in accordance with long-standing Government of Canada MOUs. This new MOU will be supported by the *CBSA Governance Model: Access and Use of the Automated Criminal Intelligence Information System* (see Annex D) as well as associated Operational Bulletins (OB), Standard Operating Procedures (SOP) developed for each investigative body, and the ACIIS mandatory training. Taken together, CBSA officers of the four investigative bodies will be made aware of the acceptable uses and applicable restrictions, when collecting, using, and disclosing information under the CISC-CBSA information-sharing framework.

The information shared under the CISC-CBSA information sharing framework must be directly related to serious and organized crime which poses a serious threat to the safety and security of Canada and may only be used to support a lawful investigation into these offences. Inclusion of an individual's personal information into the ACIIS directly links the individual or entity to serious or organized crime which may have serious consequences on their reputation, finances, or safety in the event of a privacy breach or misuse. Accordingly, the CBSA has implemented additional safeguards commensurate with the sensitivities described above in order to ensure that the terms defined in the MOU are respected. Information collected from the ACIIS is stored within closed systems of records within the custody and control of each CBSA investigative body. Both systems contain administrative safeguards such as access controls, tracking processes, and regular systems audits of user activity. A *Governance Model* provides details on the legal authorities, the ACIIS Third Party Rule, and the consistent use principle. Finally, use

of this framework will be limited to a very small group of employees within each of the four Investigative Bodies who will receive training on an ongoing basis.

Four privacy risks have been identified in Section 6 of this PIA:

1. The National Security Screening Division is not reflected in *InfoSource*.
2. Existing Personal Information Banks require updates to reflect the CBSA-CISC Information Sharing Framework.
3. Threat and Risk Assessments have not yet been undertaken for all CBSA databases housing personal information collected from partner agencies.
4. Record retention schedules for the CBSA databases described above have not yet been applied.

Privacy risk mitigation strategies for each of the risks identified above can be found in the PIA Action Plan (Annex C)

This PIA is designed to harmonize with the RCMP's *Privacy Impact Assessment of the Automated Criminal Intelligence Information System (2016)*.

ABBREVIATIONS AND ACRONYMS

ACIIS	Automated Criminal Intelligence Information System (CISC)
ATIP	Access to Information and Privacy
CBSA	Canada Border Services Agency
CIIMS	Criminal Investigations Information Management System (CBSA)
CISC	Criminal Intelligence Service Canada
COR	Class of Record
GOC	Government of Canada
GSP	Government of Canada Security Policy
HQ	Headquarters
ID	Identification
IIS	Intelligence Information System (CISC)
IMS	Intelligence Management System (CBSA)
ISA	Information Sharing Agreement
IT/IM	Information Technology/Information Management
MOU	Memorandum of Understanding
NCMS	National Case Management System (CBSA)
OPC	Office of the Privacy Commissioner of Canada
PI	Personal Information
PIA	Privacy Impact Assessment
PIB	Personal Information Bank
STS	Secure Tracking System (CBSA)
TBS	Treasury Board Secretariat
TRA	Threat and Risk Assessment
VPN	Virtual Private Network

DEFINITIONS

Action Plan	The Action Plan describes the steps that the Program will take to address risks that have been identified by ATI and Privacy Division, OPC and TBS.
Administrative purpose	The <i>Privacy Act</i> defines an “administrative purpose” to be the use of an individual’s personal information in a decision-making process that directly affects that individual.
Confidentiality	The Government Security Policy (2002) defines “confidentiality” to be the attribute that information must not be disclosed to unauthorized individuals, because of the resulting injury to national or other interests, with reference to specific provisions of the <i>Access to Information Act</i> and the <i>Privacy Act</i> .
Consistent use	Is a use that has a reasonable and direct connection to the original purpose(s) for which the information was obtained or compiled. This means that the original purpose and the proposed purpose are so closely related that the individual would expect that the information would be used for the consistent purpose, even if the use is not spelled out.
Data Matching	The <i>Policy on Privacy Protection</i> defines “data matching” as a comparison of personal data obtained from a variety of sources, including personal information banks, for the purpose of making decisions about the individuals to whom the data pertains. Data matching is a specialized activity involving the collection, use and disclosure of personal information that is subject to the various requirements of the <i>Privacy Act</i> .
Info Source	Is a series of annual Treasury Board Secretariat publications in which government institutions are required to describe their institutions, program responsibilities and information holdings, including PIBs and classes of personal information. The descriptions are to contain sufficient clarity and detail to facilitate the exercise of the right of access under the <i>Privacy Act</i> . Data-matching activities, use of the SIN and all activities for which privacy impact assessments were conducted have to be cited in <i>Info Source</i> PIBs, as applicable. The <i>Info Source</i> publications also provide contact information for government institutions as well as summaries of court cases and statistics on access requests.
Intelligence	The end product of information that has been subjected to the intelligence process and reveals the scope and dimension of organized or serious crime, and its direct or indirect participants.
Lead	Information received or collected from CBSA officials, or the public or other external sources that contain allegations of contraventions or criminal offences committed or planned against the various acts and legislation that protect Canadian public safety and national security.
Organized Crime	A group, however organized, that: <ul style="list-style-type: none"> - is composed of three or more persons in or outside Canada; - has as one of its main purposes or main activities the facilitation or commission of one or more serious offenses that, if committed, would likely result in the direct or indirect receipt of a material benefit, including a financial benefit, by the group or by any of the persons

	<p>who constitute the group; and,</p> <ul style="list-style-type: none"> - does not include a group of persons that forms randomly for the immediate commission of a single offence.
Operational Bulletin	Updates about policy and procedural changes that impact front-line work distributed through the CBSA Intranet.
Personal Information	Information about an identifiable individual as defined in section 3 of the <i>Privacy Act</i> . This definition, although lengthy, is not exhaustive, as indicated by the introductory phrase, "including, without restricting the generality of the foregoing". Information that is not specifically mentioned in the list may still be included in the definition of personal information if it qualifies as "information about an identifiable individual".
Personal Information Bank	Is a description of personal information that is organized and retrievable by a person's name or by an identifying number, symbol or other particular assigned only to that person. The personal information described in the personal information bank has been used, is being used, or is available for an administrative purpose and is under the control of a government institution.
Privacy	The Office of the Privacy Commissioner of Canada describes "privacy" as "... the right to control access to one's person and information about one's self. The right to privacy means that individuals get to decide what and how much information to give up, to whom it is given, and for what uses."
Third Party Rule	When a document is the property of an agency or department and should not be reclassified or disseminated without prior consent of the originator. The information must be stored, transmitted, and safeguarded in accordance with its classification level, as outlined in the Government Security Policy and the originator's security policies. If access is requested under <i>the Access to Information Act</i> or the <i>Privacy Act</i> , no decision should be taken without prior consultation with the originator, as the information may be subject to exemptions.
Serious Crime	Offences defined under the <i>Criminal Code</i> with penalties of 5 years or more, or offences defined under the <i>Immigration and Refugee Protection Act</i> (IRPA) with penalties of 10 years or more.

SECTION 1 - OVERVIEW AND INITIATION

1.1 Report Objectives

This report is a Privacy Impact Assessment (PIA) on the disclosure of publicly available court information by the CBSA to the CISC, and the collection of serious or organized crime intelligence in the CISC's ACIIS system by CBSA investigative bodies. Its objectives are to:

- review the business processes in order to identify the data flow of personal information;
- analyze the collection, use, disclosure and retention of personal information;
- determine if there are privacy risks associated with the CBSA-CISC information sharing; and,
- recommend strategies to mitigate or eliminate these risks.

The information presented in this report complies with all TBS policy requirements, particularly the *Directive on Privacy Impact Assessments*. It reflects the state of the initiative in February 2017.

1.1 Government Institution: Canada Border Services Agency, Programs Branch

Government Official Responsible for the
Privacy Impact Assessment

Caroline Xavier

Vice-President, Operations Branch

Head of the government institution / Delegate for
section 10 of the *Privacy Act*

Dan Proulx

Director, Access to Information and Privacy Division

1.2 Name of Program or Activity of the Government Institution:

CBSA-CISC Information Sharing Framework

1.3 Description of Program or Activity:

Program Activity: Risk Assessment

The Risk Assessment program “pushes the border out” by seeking to identify high-risk people, goods and conveyances as early as possible in the travel and trade continuum to prevent inadmissible people and goods from entering Canada. This benefits the travelling public and the trade community by enabling the Agency to focus its examination and interdiction activities on high-risk people and goods, thereby facilitating the entry of low-risk travellers and goods. The Agency uses a variety of threat and risk assessment methodologies, intelligence and supporting technologies to identify potential risks to the security and safety of people and goods.

Sub-Activity: Intelligence

The Intelligence Program collects, analyzes and distributes actionable intelligence regarding people, goods, shipments or conveyances bound for or leaving Canada to help the CBSA and other law enforcement partners identify people, goods, shipments or conveyances that may be inadmissible or pose a threat to the security of Canada. CBSA officers located within Canada, at ports of embarkation or at posts abroad assess information collected from a wide range of sources. In addition, the CBSA provides timely, accurate, strategic, operational and tactical

intelligence advice to government authorities, like-minded counterpart nations and stakeholders related to threats to national security, including information on terrorism, weapons proliferation, war crimes, organized crime, smuggling, immigration fraud and irregular migration, fraudulent documentation and border enforcement. Intelligence products such as lookouts, alerts, scientific reports and threat and risk assessments inform, support and enhance the Agency's screening and targeting capabilities and other CBSA programs (such as Admissibility Determination, Criminal Investigations and Immigration Enforcement). A lookout is reliable, accurate and actionable intelligence on actual or suspected infractions or criminal activities that may result in the interception of inadmissible people. A lookout takes the form of an electronic file record. A lookout "hit" will "flag" or identify particular individuals, including corporations, and specific goods, conveyances or shipments. A lookout "hit" requires a mandatory referral to a secondary examination.

Sub-Activity: Security Screening

The Security Screening Program is responsible for the security screening of foreign nationals who have been referred to the CBSA by an Immigration, Refugee and Citizenship Canada (IRCC) visa officer abroad or in Canada, who are seeking to come to Canada as a permanent resident, temporary resident (e.g. visitor) or refugee, or are already in Canada and seeking to remain as a temporary or permanent resident.

The CBSA is responsible for ensuring that there are no security concerns related to the individual seeking entry to Canada (e.g. counter terrorism, counter espionage, war crimes, crimes against humanity and organized crime) and, based on a thorough screening exercise (including the review of information and intelligence from a wide variety of internal and external sources), makes a recommendation to IRCC on the admissibility of the individual. This program is also responsible for determining the admissibility of senior diplomats being posted to Ottawa to ensure that they meet the admissibility requirements of the *Immigration and Refugee Protection Act*.

Program Activity: Criminal Investigations

Under the Criminal Investigations program, the CBSA protects the integrity of border-related legislation and contributes to public safety and Canada's economic security by investigating and pursuing the prosecution of travellers, importers, exporters and/or other persons who commit criminal offences in contravention of Canada's border-related legislation.

CBSA investigators review potential border legislation violations and gather evidence using a variety of investigative techniques, including search warrants, production orders and digital forensic analysis. These violations include criminal offences under the *Customs Act*, *Immigration and Refugee Protection Act*, various food, plant and animal legislations, and other border-related legislation. In conjunction with the Public Prosecution Service of Canada, the CBSA pursues the prosecution of individuals or business entities who violate Canada's border-related legislation.

Program Activity: Immigration Enforcement

The Immigration Enforcement Program determines whether foreign nationals and permanent residents who are or may be inadmissible to Canada are identified and investigated, detained, monitored and/or removed from Canada.

Foreign nationals and permanent residents of Canada believed to be inadmissible are investigated and may have a report written against them by a CBSA inland enforcement officer. Depending on the type of inadmissibility, the merits of the report are reviewed by either a Minister's Delegate or an

independent decision maker at the Immigration and Refugee Board of Canada (IRB) where a CBSA hearings officer represents the Minister of Public Safety. Subsequent to this review, a removal order may be issued against the foreign national or permanent resident in question. Removal orders issued against refugee claimants are conditional and do not come into force until the claim against the removal order is abandoned, withdrawn or denied by the IRB.

Sub-Activity: Immigration Investigations

The Immigration Investigations Program investigates reports of, and arrests foreign nationals and permanent residents already in Canada who are or may be inadmissible to Canada as defined by the *Immigration and Refugee Protection Act*.

Investigation techniques can include data analysis of information collected regarding an individual's immigration application, physical surveillance to locate fugitive inadmissible persons and field searches of residences and belongings for evidence. Depending on the type of inadmissibility and the status of the person in question, inadmissibility reports are reviewed by either a Minister's Delegate or the Immigration and Refugee Board of Canada. When a person fails to appear for an immigration proceeding such as an examination, admissibility hearing or removal interview, a warrant for their arrest may be issued. Warrants may also be issued against a foreign national or permanent resident where a CBSA inland enforcement officer has reasonable grounds to believe that they are inadmissible to Canada.

1.4 Classes of Records

<http://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/pia-efvp/atip-aiprp/infosource-eng.html>

Intelligence Program

Description: Describes records related to intelligence activities concerning individuals and entities that are of interest to the CBSA in connection to smuggling and contraband, irregular migration, immigration fraud, and inadmissibility and terrorism in support of CBSA's border enforcement mandate.

Note: Records may be found in the following systems: the Intelligence Management System (IMS), the Support System for Intelligence (SSI), the Integrated Customs Enforcement System (ICES), the Field Operations Support System (FOSS), the National Case Management System (NCMS), the Global Case Management System (GCMS) and the Canadian Police Information Center (CPIC).

Document Types: Policies, procedures, Operational Bulletins, National Directives, Alerts, Bulletins, Reports, Threat Assessments, charts, case files, Lookouts, operational and tactical intelligence analyses, screening aids, training strategies and course material, briefing material, question period cards, manuals, Memoranda of Understanding (MOU), Letters of Intent (LOI) and Written Collaborative Agreements (WCA).

Record Number: CBSA ENF 1401

Criminal Investigations Program

Description: Describes records related to the investigation of individuals and entities suspected of committing offences against Canada's border legislation, such as the *Customs Act* and/or the *Immigration and Refugee Protection Act (IRPA)*, and any subsequent or related prosecution.

Note: Records may be found in the following systems: Criminal Investigations Information Management System (CIIMS), the Intelligence Management System (IMS), the Integrated Customs Enforcement System (ICES), the Field Operations Support System (FOSS), the National Case Management System (NCMS), the Global Case Management System (GCMS), the Automated Import Reference System (AIRS), the Accelerated Commercial Release Operations Support System (ACROSS) and the Canadian Police Information Center (CPIC).

Document Types: Policies/Directives, procedures and functional guidance, manuals, strategies, budget/finance information, performance frameworks and metrics, statistics, training strategies and course material, business cases, Memoranda to Cabinet (MC), Treasury Board Submissions, Memoranda of Understanding (MOU), Written Collaborative Agreements (WCA), Letters of Intent (LOI), Production Orders, Search Warrants, Arrest Warrants, Forms (Charge Forms, Evidence Seizure Receipt, Notice of Ascertained Forfeiture, Statement of Goods Seized, Exhibit Control, Notice of Ascertained Forfeiture, Notice of Penalty Assessment, Notice to Crown Counsel), operational bulletins, plans and reports and briefing material.

Record Number: CBSA ENF 123

Immigration Investigation Program

Description: Describes records related to investigations into Foreign Nationals (FN) or Permanent Residents (PR) who may be inadmissible to Canada under the Immigration and Refugee Protection Act (IRPA).

Note: Records may be found in the following systems: the Field Operations Support System (FOSS), the National Case Management System (NCMS) and the Canadian Police Information Center (CPIC).

Document Types: Admissibility/Inadmissibility reports, forms (Vienna Convention Rights Form, Notice of Seizure, Notice of Arrest, Departure Order, Deportation Order, Exclusion Order), Warrants, case files, policies/directives, procedures, operational bulletins, manuals, discussion papers, Memoranda of Understanding (MOU), performance framework material, training strategies and course material, briefing notes, issue sheets and question period cards.

Record Number: CBSA ENF 130

The CBSA is currently revising the structure and content of its *InfoSource* Chapter. This compliance risk with the *Access to Information Act* has been identified in Section 6 - Summary of Analysis and Recommendations, below.

1.5 Personal Information Banks

<http://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/pia-efvp/atip-aiprp/infosource-eng.html>

Intelligence Program:

Description: This bank describes information that is about individuals suspected of involvement in contraband smuggling, money laundering, terrorist financing, immigration fraud, irregular migration, human smuggling and/or trafficking, terrorism, or other border related enforcement and security concerns. Also includes information on individuals suspected of being inadmissible to Canada.

Personal information may include name, contact information, biographical information, biometric information, citizenship status, credit information, criminal checks/history, date of birth, educational information, financial information, travel/identity documents, personal identification numbers, physical attributes, place of birth, signature, import/export information, customs infractions and/or seizures, traveller history and immigration violations.

Note: In addition to the requirements specified on the Treasury Board of Canada Secretariat Personal Information Request form, individuals requesting information described by this bank must provide the incident and location. Personal Information may be stored in the following systems: the Intelligence Management System (IMS), the Support System for Intelligence (SSI), the Secure Tracking System (STS), the Integrated Customs Enforcement System (ICES), the National Case Management System (NCSM), the Field Operations Support System (FOSS), the Global Case Management System (GCMS) and the Canadian Police Information Center (CPIC).

Class of Individuals: General Public.

Purpose: Personal information is collected pursuant to the *Customs Act*, the *Immigration and Refugee Protection Act (IRPA)*, the *Customs Tariff*, the *Excise Act*, the *Excise Tax Act*, the *Export & Import Permits Act*, the *Controlled Drugs and Substances Act (CDSA)* and the *Proceeds of Crime (Money Laundering) & Terrorist Financing Act* for the purposes of obtaining information on persons who are suspected of border related illegal activities, including contraband smuggling and immigration violations.

Consistent Uses: The information may be disclosed internally to the *CBSA Operations and Programs Branches* for the purposes of enforcement, security, audit and evaluation, briefing senior management, and policy, procedural, and training development. The information may be disclosed externally to ~~Citizenship and Immigration Canada (CIC)~~ Immigration, Refugees and Citizenship Canada (IRCC), the Canadian Security Intelligence Service (CSIS) and the Immigration and Refugee Board (IRB) for the purposes of administering and enforcing the *Immigration and Refugee Protection Act (IRPA)*; refer to: Immigration Case File CIC PPU 042, Canadian Security Intelligence Service Investigational Records CSIS PPU 045, Immigration Division Case Files IRB PPU 140, Health Canada for the purposes of administering and enforcing the *Controlled Drugs and Substances Act (CDSA)*; refer to: Inspectorate - Medical Devices HC PPU 405, Inspectorate - Natural Health Products HC PPU 406, Inspectorate - Pharmaceutical Drugs HC PPU 407M, Inspectorate - Biologics & Radiopharmaceuticals HC PPU 408, the Public Prosecution Service of Canada and the Department of Justice (DOJ) for the purposes of prosecution and/or appeals; refer to: Prosecutions and Prosecution-Related Activities PPSC PPU 002, Prosecution and Related Criminal Matters JUS PPU 015, the Royal Canadian Mounted Police (RCMP) for the purposes of law enforcement; refer to: Operational Case Records RCMP PPU 005 and ~~Department of Foreign Affairs, Trade and Development (DFAIT)~~ Global Affairs Canada (GAC) for the purposes of export control. The information may also be disclosed externally with various Foreign Governments subject to multilateral Treaties, Mutual Legal Assistance Treaties, or Written Collaborative Agreements (WCA), Interpol and municipal/provincial/territorial law enforcement agencies for the purposes law enforcement.

Retention and Disposal Standards: Customs Information: Records will be retained for five years and then are destroyed; **Immigration Information:** Under Development

RDA Number: Customs Information: 2000/033; **Immigration Information:** 2006/004

Related Record Number: CBSA ENF 137, CBSA ENF 1401

TBS Registration: 005187

Bank Number: CBSA PPU 035

Criminal Investigations Program:

Description: This bank describes information that is about individuals subject to criminal investigation by the CBSA. Personal information may include photographs, name, contact information, biographical information, biometric information, citizenship status, credit information, criminal checks/history, date of birth, date of death, educational information, financial information, personal identification numbers, physical attributes, place of birth, place of death, signature, identity/travel document, residence history, phone records, computer records, caution flags, business records, import/export information, customs infractions and seizures, immigration violations and offences, travel history.

Note: In addition to the requirements specified on the Treasury Board of Canada Secretariat Personal Information Request form, individuals requesting information described by this bank must provide the incident and location. Personal information may be stored in the following systems: the Criminal Investigations Information System (CIIMS), the Intelligence Management System (IMS), the Integrated Customs Enforcement System (ICES), the Automated Import Reference System (AIRS), the Accelerated Commercial Release Operations Support System (ACROSS), the Field Operations Support System (FOSS), the Global Case Management System (GCMS), the National Case Management System (NCMS), the Secure Tracking System (STS) and the Canadian Police Information Centre (CPIC).

Class of Individuals: General Public.

Purpose: Personal information is collected pursuant to the *Immigration and Refugee Protection Act (IRPA)*, the *Customs Act*, the *Customs Tariff*, the *Excise Act*, *Export and Import Permits Act* and the *Criminal Code of Canada* for the purposes of law enforcement.

Consistent Uses: The information may be disclosed internally to the *CBSA Operations Branch* for the purposes of law enforcement, for purposes of detection, suppression and prevention of offences and for the purposes of quality assurance, evaluation, Program integrity and to brief senior management. The information may be disclosed externally to the Public Prosecution Service of Canada and the Department of Justice (DOJ) for the purposes of prosecution and/or appeal purposes; refer to: Prosecutions and Prosecution-Related Activities PPSC PPU 002 and Prosecution and Related Criminal Matters JUS PPU 015, and to the Royal Canadian Mounted Police (RCMP) for the purposes of law enforcement; refer to: Operational Case Records RCMP PPU 005. The information may also be disclosed externally to Foreign Governments subject to multilateral Treaties or Written Collaborative Agreements (WCA), provincial attorney generals (crown attorneys), law enforcement bodies and detaining authorities for the purposes of law enforcement. Information may also be disclosed externally to municipal/provincial/territorial law enforcement agencies and Interpol for the purpose of law enforcement.

Retention and Disposal Standards: Customs Information: Records will be retained for seven five years and then are destroyed. **Immigration Information:** Under Development.

RD Number: Customs Information: 2000/033; **Immigration Information:** 2006/004

Related Record Number: CBSA ENF 123

TBS Registration: 20140079

Bank Number: CBSA PPU 1402

Immigration Investigations Program:

Description: This bank describes information that is used in support of the Immigration Investigations Program, including the management of immigration arrest warrants, the preparation and confirmation of inadmissibility reports, supporting material for inadmissibility hearings, detention reviews and Immigration Appeal Division appeal hearings from visa refusal decisions or removal orders. Personal information may include name, contact information, biographical

information, biometric information, citizenship status, credit information, criminal checks/history, date of birth, place of birth, educational information, financial information, physical attributes, employee personnel information, medical information, photos, signature, travel documentation, travel history and personal identification numbers.

Note: In addition to the requirements specified on the Treasury Board of Canada Secretariat Personal Information Request form, individuals requesting information described by this bank must provide the immigration client identification number. Personal information may be stored in the following systems: the Field Operations Support System (FOSS), the Global Case Management System (GCMS), the National Case Management System (NCMS), the Secure Tracking System (STS), the Confirmation and Tracking System (CATS) and the Canadian Police Information Centre (CPIC).

Class of Individuals: Foreign Nationals (FN) and Permanent Residents (PR).

Purpose: Personal information is collected pursuant to the *Immigration and Refugee Protection Act (IRPA)* for the purposes of the administration and enforcement of *IRPA* and related immigration legislation and regulations.

Consistent Uses: The information may be disclosed internally with the *CBSA Operations and Programs Branches* for the purposes of enforcing the *Immigration and Refugee Protection Act (IRPA)*, including the “*Wanted by the CBSA*” initiative, audit and evaluation, briefing senior management and policy, procedural, and training development. The information may be disclosed externally to ~~Citizenship and Immigration Canada (CIC)~~ Immigration, Refugees and Citizenship Canada (IRCC) for the purposes of administering Immigration and Refugee Programs; refer to: Immigration Case File CIC PPU 042, to the Royal Canadian Mounted Police (RCMP) for the purpose of immigration law enforcement; refer to Operational Case Records RCMP PPU 005. The information may also be disclosed externally with various Foreign Governments subject to multilateral Treaties, Mutual Legal Assistance Treaties, or Written Collaborative Agreements (WCA) for the purposes of administering and enforcing immigration and citizenship laws. Information may also be disclosed externally to municipal/provincial/territorial law enforcement agencies and Interpol for the purposes of immigration law enforcement.

Retention and Disposal Standards: Under Development.

RDA Number: Customs Information: 2000/033; Immigration Information: 2006/004

Related Record Number: CBSA ENF 137, CBSA ENF 127, CBSA ENF 130

TBS Registration: 20140077

Bank Number: CBSA PPU 1403

The CBSA is currently revising the structure and content of its *InfoSource* Chapter. This compliance risk with the *Access to Information Act* has been identified in Section 6- Summary of Analysis and Recommendations, below.

1.6 Legal Authority for Program or Activity:

CBSA derives its authorities from the *Canada Border Services Agency Act*, its program legislation, and related legislation, including, but not limited to the following:

CBSA Authority to Collect CISC Data:

- The *Privacy Act* (s.4) requires that no personal information may be collected by a government institution unless it relates directly to an operating program or activity of the institution.

- The *Canada Border Services Agency Act* (s. 5) provides the mandate of the CBSA as “providing integrated border services that support national security and public safety priorities” by (a) supporting the administration or enforcement, or both, as the case may be, of the program legislation.
 - “Program Legislation”, within the *CBSA Act*, is defined as “any other Act of Parliament, or any instrument made under it, or any part of such an Act or instrument” (a) “that the Governor in Council or Parliament authorizes the Minister, the Agency, the President, or an employee of the Agency to administer and enforce, including the *Customs Act*...[and] the *Immigration and Refugee Protection Act*.”
- The *Canada Border Services Act* (s. 9(2)) authorizes the President of the Agency to designate a person or class of persons as officers.
- The *Immigration and Refugee Protection Act* includes a number of grounds for inadmissibility for participating in or being a member of an organized crime group, including:
 - Serious Criminality (s.36)
 - Organized Criminality (s.37)
- The *Customs Act* includes a number of offences which are commonly violated by organized crime units related to the illicit importation of goods, including:
 - Smuggling (s. 159)

CISC Authority to Disclose Data to CBSA:

- The *Privacy Act* (s. 8(2)) allows for personal information to be disclosed without the consent of the individual to whom it relates for the following purposes:
 - Consistent Use (8(2)(a)): when the purpose for which the CBSA would use the information is clearly and directly connected to the purpose for which it is collected. In the case of ACIIS, CISC must be satisfied that the CBSA will only use the information to further a lawful investigation in relation to organized crime. This consistent use is currently detailed in RCMP Personal Information Bank PPU 005: Operational Case Records.
 - Investigative Use (8(2)(e)); when an investigative body of the CBSA, specified by Schedule II of the *Privacy Regulations*, has provided a written request to the originator detailing the law it is seeking to enforce or the lawful investigation it seeks to carry out and describes the information being requested.
 - Schedule II of the *Privacy Regulations* designates specific areas of the CBSA with “Investigative Body” status for the purpose of 8(2)(e):
 - Criminal Investigations Division,
 - Inland Enforcement Division
 - Intelligence & Targeting Operations Directorate
 - Schedule II of the *Privacy Regulations* does not include the National Security and Screening Division.
 - The *Public Service Rearrangement and Transfer of Duties Act* states that if a unit has the same powers, duties or functions of its predecessor unit, those powers, duties or functions are transferred to the new unit. This means that if the requesting unit is a legacy unit of one listed in the *Privacy Regulations*, then they are considered to have IBD status.
 - The National Security Screening Division (NSSD) is a legacy unit of the Intelligence & Targeting Operations Directorate currently listed in the *Privacy Regulations* and are considered to have IBD status.

CBSA Authority to Use CISC Data:

- The *Privacy Act* (s. 7(b)) requires that “personal information under the control of a government institution shall not...be used by the institution except...(b) for a purpose for which the information may be disclosed to the institution under s. 8(2).”
 - As articulated in the CBSA Governance Model, information may only be used for the purpose for which it was collected: to support lawful investigations into serious and organized crime. Any secondary use or disclosure requires a CBSA investigator to obtain a written consent from the originating party or request a disclosure under a different provision under s. 8(2) of the *Privacy Act*.

CBSA Authority to Disclose Publicly Available Information:

- The *Privacy Act* (s. 69(2)) excludes publicly available information from the use (s.7) and disclosure (s.8) restrictions. Published court records are considered publicly available by default unless the judiciary has imposed specific measures to prevent publication.

CBSA Authority to Disclose Personal Information upon Request:

- The *Privacy Act* (s. 8(2)) allows for personal information to be disclosed without the consent of the individual to whom it relates for the following purposes:
 - Investigative Use (8(2)(e)); when the requesting agency, listed in Schedule II of the *Privacy Regulations*, has provided a written request to the CBSA detailing the law it is seeking to enforce or the lawful investigation it seeks to carry out and describes the information to be disclosed.
 - Under an arrangement or agreement (s. 8(2)(f); when an arrangement or agreement is in place between the Government of Canada and a province and the information will be used to carry out a lawful investigation.
 - The Government of Canada, represented by the Attorney General, has information sharing Memoranda of Understanding with the Attorney General of each province signed in 1982 to enable sharing of personal information. These arrangements do not contain the same privacy safeguards as found within contemporary CBSA MOUs. This has been identified as a privacy risk in section 6 of the PIA.
- The *Customs Act* (s. 107(5)(a)) permits the disclosure of customs information to a peace officer if the official who is disclosing the information has reasonable grounds to believe that the information relates to the alleged indictable offence and will be used in the investigation or prosecution of said offence.

1.7 Summary of the Project, Initiative, or Change:

The purpose of this PIA is to identify potential privacy risks related to the collection, use and disclosure of personal information shared between the Canada Border Services Agency (CBSA) and the Criminal Intelligence Service of Canada (CISC) and the recommended strategies to mitigate potential privacy risks related to the collection, use and disclosure of personal information among partner agencies. This project is scheduled for implementation in early 2017 upon signature of the CBSA-CISC Memorandum of Understanding (Annex G).

The CBSA's investigative bodies will collect personal information from the Automated Criminal Intelligence Information System (ACIIS), through the Intelligence Information System (IIS) query tool, to support ongoing lawful investigations of customs and immigration-related offences with a nexus to organized crime by directly accessing the ACIIS. If relevant information is found, the CBSA officer must follow-up with the originating member agency, through a written request detailing the purpose of the investigation, to seek consent to use this information. The scope of this PIA is focused on information sharing between the CBSA and CISC. It does not examine the use of this information in the operational context of each Investigative Body, as this will be examined in PIAs specific to the function of each investigative body. The CBSA recognizes that it has a significant gap in its current PIA framework and has identified this as a privacy risk in Section 6 below.

The CBSA will also share and maintain publically available court information relating to serious or organized crime (and the related CIIMS case number) with ACIIS partner agencies. Authorized CISC member law enforcement agencies may access this information within ACIIS and may provide a written request to the CBSA for additional information to support their own lawful investigations. The CBSA will evaluate each request on a case-by-case basis in accordance with the *Policy on the Disclosure of Personal Information: Section 8 of the Privacy Act* or the *Policy on the Disclosure of Customs Information: Section 107 of the Customs Act*; depending on the type of information requested.

ACIIS is Canada's primary law enforcement database for serious and organized crime. It contains sensitive financial, biometric, and biographic personal information as well as detailed descriptions related to suspects' criminal history, associations, and profile. The National Executive Committee (NEC) of the CISC will provide direct access to ACIIS unrestricted data to select officers within each of the CBSA's four investigative bodies (Inland Enforcement Division, Intelligence Operations Division, Criminal Investigations Division, and National Security Screening Division). As a Category II(a) member, the CBSA has been granted access, based on the Agency's responsibilities and legislative mandate, conditional on the use of this data being limited to criminal information/intelligence concerning serious and/or organized crime in accordance with the ACIIS policy and Regulations and the governance framework. The CBSA has developed a *Governance Model* to act as an overview for officers to ensure that the Agency is supporting the CISC national strategy to combat serious and organized crime as well as abiding by its commitments under the CISC governance framework. The *Governance Model* will be supplemented by specific Operational Bulletins and/or Standard Operating Procedures to provide practical guidance to officers collecting, using, and disclosing personal information under the CBSA-CISC Information Sharing Framework.

Four Part Test of Necessity, Effectiveness, Proportionality, and Minimal Privacy Intrusion

Serious and organized criminal activity is a multi-faceted problem that poses a significant threat to public safety and negatively affects the daily lives of Canadians. Tied to illegal activities such as drug smuggling, money laundering, theft, and human trafficking, organized crime groups and individual actors have a violent and corrupting effect extending beyond any single jurisdiction. Beyond the immediate effect of the crimes themselves, organized crime entails a number of secondary effects such as greater costs for law enforcement, justice, and corrections as well as higher insurance premiums and banking fees. Many criminal organizations operate throughout Canada and across international boundaries, have significant resources, and are constantly adapting to exploit new opportunities. Accordingly, it is extremely difficult for isolated law enforcement to differentiate isolated acts by independent actors from coordinated operations by sophisticated organized crime groups. Information sharing amongst law enforcement agencies is a **necessary** tool to identify, intercept, and ultimately dismantle organized

crime groups by enabling an intelligence-led response to focus resources across multiple jurisdictions to target the leadership of these groups.

Created in 1970, the CISC has a proven record demonstrating the effectiveness of information sharing among municipal, provincial, and federal law enforcement agencies. Previous national tactical strategies have focused on the dissolution of Outlaw Motorcycle Gangs, illicit offshore gambling enterprises, child pornography rings, and drug manufacturing/distribution groups. The CISC is **effective** at analysing and defining the problem to enable larger coordinating bodies, such as the Canadian Integrated Response to Organized Crime (CIROC) and the Canadian Association of Chiefs of Police (CACP), to commit resources at the strategic level to support tactical operations among partner organizations at the Federal, Provincial and Territorial levels.

The CISC governance framework, as well the CBSA *Governance Model*, is designed to ensure that information contained within the ACIIS database is limited exclusively to persons or entities directly involved in serious organized crime. Each disclosing institution is responsible for identifying the reliability of the information, in accordance with regulation 7 of the *CISC Regulations*, and the CBSA *Governance Model* requires that secondary verifications be performed before any administrative action is taken. Moreover, each party is bound by restrictions to seek written authorization of the originating party before disclosing the information onward or using the information to investigate another crime. Information sharing on organized crime groups, and the resultant law enforcement efforts which may follow, is considered by the CBSA to be **proportional** because the violence, financial loss, and other negative societal effects caused by serious and organized crime overwhelmingly supersedes the reasonable expectation of privacy of individuals suspected of engaging in these activities.

The CISC is designed in a privacy-sensitive manner by providing the **minimal** amount of personal information necessary to enable investigators and analysts to identify partners with relevant information and facilitate communication among these bodies. The originating body maintains the discretion for disclosing additional information upon receipt of a written request. The requesting partner remains bound by a strictly enforced “Third-Party Rule” regime to prevent the onward disclosure or secondary use of information without the consent of the originator. Finally, information sharing is among the **least invasive** tools within an investigator’s toolkit. Validating the reliability of information amongst a larger pool of trusted partners, within the law enforcement community, prevents more invasive investigative techniques (such as electronic surveillance, physical monitoring, or infiltration by undercover officers) from being employed based on incomplete or inaccurate information.

A number of risks have been identified in this Privacy Impact Assessment (PIA), as reflected in Section 6: *Summary of Risks and Recommendations*. CBSA Senior Management has acknowledged these risks and has developed an Action Plan to implement mitigation strategies for each risk. The CBSA expects that these mitigation strategies will be fully implemented in accordance with the commitments detailed in the *PIA Action Plan* (Annex C)

SECTION 2 - RISK AREA IDENTIFICATION AND CATEGORIZATION

2.1	Type of Initiative	Level of Risk
1.1	Initiative that does NOT involve a decision about an identifiable individual Personal information is used strictly for statistical / research or evaluations including mailing list where no decisions are made that directly have an impact on an identifiable individual. The Directive on PIA applies to administrative use of personal information. The Policy on Privacy Protection requires that government institutions establish an institutional Privacy Protocol for addressing non-administrative uses of personal information.	<input type="checkbox"/> 1
2.2	Administration of Programs / Activity and Services Personal information is used to make decisions that directly affect the individual (i.e. determining eligibility for programs including authentication for accessing programs/services, administering program payments, overpayments, or support to clients, issuing or denial of permits/licenses, processing appeals, etc.)	<input type="checkbox"/> 2
2.3	Compliance / Regulatory investigations and enforcement Personal information is used for purposes of detecting fraud or investigating possible abuses within programs where the consequences are administrative in nature (i.e. a fine, discontinuation of benefits, audit of personal income tax file or deportation in cases where national security and/or criminal enforcement is not an issue).	<input type="checkbox"/> 3
2.4	Criminal investigation and enforcement / National Security Personal information is used for investigations and enforcement in a criminal context (i.e. decisions may lead to criminal charges/sanctions or deportation for reasons of national security or criminal enforcement).	<input checked="" type="checkbox"/> 4

Details: ACIS data will be used by CBSA investigative bodies to support lawful investigations into serious and organized crime. The outcome of these activities may lead to criminal prosecution or removal from Canada.

2.2	Type of Personal Information Involved and Context	Level of Risk
2.1	Only personal information, with no contextual sensitivities, collected directly from the individual or provided with the consent of the individual for disclosure under an authorized program.	<input type="checkbox"/> 1
2.2	Personal information, with no contextual sensitivities after the time of collection, provided by the individual with consent to also use personal information held by another source.	<input type="checkbox"/> 2
2.3	Social Insurance Number, medical, financial or other sensitive personal information and/or the context surrounding the personal information is sensitive. Personal information of minors or incompetent individuals or involving a representative acting on behalf of the individual.	<input type="checkbox"/> 3
2.4	Sensitive personal information, including detailed profiles, allegations or suspicions, bodily samples and/or the context surrounding the personal information is particularly sensitive.	<input checked="" type="checkbox"/> 4

Details: The CBSA will collect sensitive financial, biometric and biographic personal information as well as detailed descriptions related to criminal history, associations & affiliations, and other contextual information.

2.3 Initiative Partners and Private Sector Involvement	Level of Risk
3.1 Within the CBSA (amongst one or more programs within the CBSA)	<input type="checkbox"/> 1
3.2 With other federal institutions	<input type="checkbox"/> 2
3.3 With other or a combination of federal/ provincial and/or municipal government(s)	<input checked="" type="checkbox"/> 3
3.4 Private sector organizations or international organizations or foreign governments	<input checked="" type="checkbox"/> 4

Details: The proposed initiative will result in an agreement between the CBSA and the CISC, the organization managing the ACIIS database and policies. The ACIIS is accessible to 400 domestic federal, provincial and municipal law enforcement agencies as well as international agencies such as Interpol.

2.4 Duration of the Initiative	Level of risk
4.1 One-time initiative Typically involves offering a one-time support measure in the form of a grant payment as a social support mechanism.	<input type="checkbox"/> 1
4.2 Short-term program An initiative that supports a short-term goal with an established "sunset" date.	<input type="checkbox"/> 2
4.3 Long-term program Existing program that has been modified or is established with no clear "sunset".	<input checked="" type="checkbox"/> 3

Details: CBSA access to the ACIIS has no expected end date.

2.5 Program Population	Level of Risk
5.1 The program affects certain employees for internal administrative purposes.	<input type="checkbox"/> 1
5.2 The program affects all employees for internal administrative purposes.	<input type="checkbox"/> 2
5.3 The program affects certain individuals for external administrative purposes.	<input checked="" type="checkbox"/> 3
5.4 The program affects all individuals for external administrative purposes.	<input type="checkbox"/> 4

Details: Information collected and used by the CBSA from ACIIS will be related to the subjects of lawful investigations who are suspected of involvement in serious or organized crime. Court records disclosed by CBSA are publically available.

2.6 Technology and Privacy	
6.1 Does the new or modified initiative involve the implementation of a new electronic system, software or application program including collaborative software (or groupware) that is implemented to support the initiative in terms of the creation, collection or handling of personal information?	Yes
6.2 Does the new or modified initiative require any modifications to IT legacy systems and / or services?	No
6.3 Does the new or modified initiative involve the implementation of one or more of the following technologies:	
6.3.1 Enhanced identification methods: This includes biometric technology (i.e. facial recognition, gait analysis, iris scan, fingerprint analysis, voice print, radio frequency identification (RFID), etc.) as well as easy pass technology, new identification cards including magnetic stripe cards, "smart cards" (i.e. identification cards that are embedded with either an antenna or a contact pad that is connected to a microprocessor and a memory chip or only a memory chip with non-programmable logic).	No
6.3.2 Use of Surveillance: This includes surveillance technologies such as audio/video recording devices, thermal imaging, recognition devices, RFID, surreptitious surveillance / interception, computer aided monitoring including audit trails, satellite surveillance etc.	No
6.3.3 Use of automated personal information analysis, personal information matching and knowledge discovery techniques: For the purposes of the <i>Directive on PIA</i> , this includes activities that involve the use of automated technology to analyze, create, compare, cull, identify or extract personal information elements. Such activities would include personal information matching, record linkage, personal information mining, personal information comparison, knowledge discovery, information filtering or analysis. Such activities involve some form of artificial intelligence and/or machine learning to uncover knowledge (intelligence), trends/patterns or to predict behaviour.	No

2.7 Personal Information Transmission	Level of Risk
7.1 The personal information is used within a closed system. No connections to Internet, Intranet or any other system. Circulation of hardcopy documents is controlled.	<input type="checkbox"/> 1
7.2 The personal information is used in system that has connections to at least one other system.	<input type="checkbox"/> 2
7.3 The personal information is transferred to a portable device or is printed. USB key, CD-ROM, laptop computer, any transfer of the personal information to a different medium.	<input checked="" type="checkbox"/> 3
7.4 The personal information is transmitted using wireless technologies.	<input type="checkbox"/> 4

Details: CBSA investigators will access the ACIIS system via the IIS interface over a secure VPN incorporating PKI cryptography from authorized workstations in secure CBSA locations across Canada.

2.8	Risk to CBSA from a Breach (Court Data)	Level of Risk
8.1	Managerial harm. Processes must be reviewed, tools must be changed, change in provider / member.	<input checked="" type="checkbox"/> 1
8.2	Organizational harm. Changes to the organizational structure, changes to the organizations decision-making structure, changes to the distribution of responsibilities and accountabilities, changes to the program activity architecture, departure of employees, reallocation of HR resources.	<input type="checkbox"/> 2
8.3	Financial harm. Lawsuit, additional moneys required reallocation of financial resources.	<input type="checkbox"/> 3
8.4	Reputation harm, embarrassment, loss of credibility. Decreased confidence by the public, elected officials under the spotlight, institution strategic outcome compromised, government priority compromised, impact on the Government of Canada Outcome areas.	<input type="checkbox"/> 4

Details: A breach of publically available court data associated to other information in either ACIIS or CIIMS may lead to the revocation of access to ACIIS as well as a loss of credibility among law enforcement partners and the general public.

2.9	Risk to Individual from a Breach (Court Data)	Level of Risk
9.1	Inconvenience.	<input checked="" type="checkbox"/> 1
9.2	Reputation harm, embarrassment.	<input checked="" type="checkbox"/> 2
9.3	Financial harm.	<input checked="" type="checkbox"/> 3
9.4	Physical harm.	<input checked="" type="checkbox"/> 4

Details: A breach of a court record not related to serious and organized crime may link the individual to these types of activities if the offence is not explicitly related to organized crime.

2.10 Risk to CBSA from a Breach (ACIIS Data)	Level of Risk
10.1 Managerial harm. Processes must be reviewed, tools must be changed, change in provider / member.	<input checked="" type="checkbox"/> 1
10.2 Organizational harm. Changes to the organizational structure, changes to the organizations decision-making structure, changes to the distribution of responsibilities and accountabilities, changes to the program activity architecture, departure of employees, reallocation of HR resources.	<input checked="" type="checkbox"/> 2
10.3 Financial harm. Lawsuit, additional moneys required reallocation of financial resources.	<input checked="" type="checkbox"/> 3
10.4 Reputation harm, embarrassment, loss of credibility. Decreased confidence by the public, elected officials under the spotlight, institution strategic outcome compromised, government priority compromised, impact on the Government of Canada Outcome areas.	<input checked="" type="checkbox"/> 4

Details: If data disclosed from the CISC's ACIIS database to CBSA investigative bodies is breached, the Director General, CISC or Executive Committee may suspend or revoke access to ACIIS or membership in CISC, in accordance with the *CISC governance framework*. Moreover, breach of information related to entities, operations, or the context of serious and organized crime investigations may have a substantial impact on the reputation of, and confidence in the CBSA both within the law enforcement community and among the public.

2.11 Risk to Individual from a Breach (ACIIS Data)	Level of Risk
10.1 Inconvenience.	<input checked="" type="checkbox"/> 1
10.2 Reputation harm, embarrassment.	<input checked="" type="checkbox"/> 2
10.3 Financial harm.	<input checked="" type="checkbox"/> 3
10.4 Physical harm.	<input checked="" type="checkbox"/> 4

Details: Data improperly collected, used, or disclosed may cause serious harm to an individual, group, or entity's reputation, finances, or safety.

SECTION 3 - ANALYSIS OF PERSONAL INFORMATION ELEMENTS

1. CBSA Data to be uploaded to ACIS:

	Category	Element	Sub-Element	Format	Purpose / Necessity	Notes
1	Biographical	Entity first name	Entity first name	E	To identify individuals in the CIIMS system	
2	Biographical	Entity second name	Entity second name	E	To identify individuals in the CIIMS system	
3	Biographical	Entity name	Entity name	E	To identify individuals in the CIIMS system	
4	Biographical	Date of Birth	Day, month, year	E	To identify individuals in the CIIMS system	
5	Criminal History	Date charges laid	NA	E	To describe criminal history	
6	Criminal History	Date concluded	NA	E	To identify when the enforcement action concluded	
7	Criminal History	Results	NA	E	To describe results of trial	Includes Act and Section against which charges were laid
8	Criminal History	Sentence	NA	E	To describe the sentence handed down	
9	Investigation	CIIMS Case Number	NA	E	Reference number in CIIMS case management system	
10	Investigation	Association with Organized Crime	NA	N/A	To conform to File Entry Criteria, as defined in part F of <i>CISC Regulations</i>	Connection with organized crime created by inference based on inclusion in ACIS

2. ACIS Data Available to CBSA:

	Category	Element	Sub-Element	Format	Purpose / Necessity	Notes
1	Biographical	Name	Surname	E	To identify individual in support of a lawful investigation	
2	Biographical	Name	Given names	E	To identify individual in support of a lawful investigation	
3	Biographical	Aliases	Aliases	E	To identify individual in support of a lawful investigation	
4	Biographical	Date of birth	Day, month, year	E	To identify individual in support of a lawful investigation	
5	Biographical	Age	NA	E	To identify individual in support of a lawful investigation	
6	Biographical	Sex	Male / female	E	To identify individual in support of a lawful investigation	
7	Biographical	Race	NA	E	To identify individual in support of a lawful investigation	Race assists to identify person(s). The CBSA encounters many persons arriving at Canada's ports of entry.
8	Physical Descriptors	Hair	Colour, length, style	E	To identify individual in support of a lawful investigation	
9	Physical Descriptors	Eye colour	Colour (e.g: Blue)	E	To identify individual in support of a lawful investigation	
10	Physical	Facial hair	Style (e.g Beard)	E	To identify individual in support of a lawful investigation	

	Category	Element	Sub-Element	Format	Purpose / Necessity	Notes
	Descriptors					
11	Physical Descriptors	Complexion	NA	E	To identify individual in support of a lawful investigation	
12	Physical Descriptors	Height	NA	E	To identify individual in support of a lawful investigation	
13	Physical Descriptors	Weight	NA	E	To identify individual in support of a lawful investigation	
14	Biographical	Marital status	Single, married	E	To identify individual with close associative ties to primary suspect	Spouse not identified unless they are suspected of involvement or complicity in primary suspect's illegal activities.
15	Biographical	Descent	African, Arab, Canadian, Caribbean, Estonian, etc.	E	To identify individual in support of a lawful investigation To establish associative ties for descent-based organized crime groups	Descent is a five-digit code which refers to the heritage or ethnicity of the subject. There are 50 descent codes.
16	Biographical	Date deceased	NA	E	To identify individual in support of a lawful investigation To close investigations against deceased individuals	Date deceased only applies for individuals who have been dead for less than twenty years, in accordance with 3(m) of the <i>Privacy Act</i> .
17	Biographical	Employment	NA	E	To support a lawful investigation as a reflection of subject's legitimate means of income To support a lawful investigation to locate an individual	May be used as a comparison against individual's lifestyle and spending habits to indicate presence of illicit source of funds.

	Category	Element	Sub-Element	Format	Purpose / Necessity	Notes
					To support a lawful investigation if employing entity is involved as an organized crime entity	
18	Biographical	Chinese Telegraphic Code ¹	NA	E	To support a lawful investigation into individuals or entities communicating in Chinese characters	
19	Biometric	Finger Print Serial	NA	E	This element may be collected by the CBSA from ACIIS if it supports a lawful investigation to help confirm the identity of the subject.	Finger Print Serial numbers are available in the Canadian Police Information Centre. The collection of this information supports the confirmation of a person's identity.
20	Criminal History	Local criminal record no.		E	To identify individual in support of a lawful investigation To facilitate written request to originating body and expedite retrieval of associated record	
21	Biographical	Net worth		E	To support a lawful investigation as a reflection of subject's legitimate means of income	

¹ CTC - recognized international numeric equivalent for Chinese names

	Category	Element	Sub-Element	Format	Purpose / Necessity	Notes
22	Biographical	Scope/sphere of influence		E	To support lawful investigation to determine geographic and social influence on others	
23	Biographical	Clothing frequently worn		E	To identify an individual subject to a lawful investigation in the field To support a lawful investigation as a reflection of subject's legitimate means of income	May be used as a comparison against individual's lifestyle and spending habits to indicate presence of illicit source of funds. Some criminal organizations wear clothing representing allegiance to the group – outlaw motorcycle gangs or street gangs.
24	Nationality	Place of birth		E	To identify individual in support of a lawful investigation To establish associative ties for descent-based organized crime groups	
25	Biographical	Base	City	E	To identify related entities within individual's sphere of influence To support a lawful investigation to locate a subject	Geo-code assigned to individual's city of operation.
26	Physical Characteristics	Physical characteristics	Scars, tattoos, piercings	E	To identify individual in support of a lawful investigation To establish membership in a group based on distinctive markings	
27	Biographical	Languages spoken		E	To identify individual in support of a lawful investigation To establish associative ties for descent-based organized crime groups To procure specialist translation services,	

	Category	Element	Sub-Element	Format	Purpose / Necessity	Notes
					where necessary	
28	Biographical	Driver's license	Number, province	E	To identify an individual in support of a lawful investigation	
29	Biographical	Country of residence		E	To establish associative ties for descent-based organized crime groups	
30	Biographical	Passport number		E	To identify individual in support of a lawful investigation	
31	Nationality	Citizenship		E	To identify individual in support of a lawful investigation	
32	Criminal History	Criminal activity		E	To identify individual in support of a lawful investigation	Activity/function/commodity to describe the suspected or confirmed criminal activity
33	Biographical	Type of ID used	Credit cards, etc.	E	To identify an individual in support of a lawful investigation	
34	Criminal History	Types of individual	Suspect, charged, person of interest, gang member, deceased person	E	To establish membership in an organized crime group To tailor investigative technique based on proximity and ranking within a group	
35	Contact	Telecomm info	Description	E	To identify individual in support of a lawful investigation To facilitate electronic surveillance, if required	
37	Contact	Telecomm info	Phone type	E	To identify individual in support of a lawful investigation To facilitate electronic surveillance, if	

	Category	Element	Sub-Element	Format	Purpose / Necessity	Notes
					required	
37	Contact	Telecomm info	Country code	E	To identify individual in support of a lawful investigation To facilitate electronic surveillance, if required	
38	Contact	Telecomm info	Area code	E	To identify individual in support of a lawful investigation To facilitate electronic surveillance, if required	
39	Contact	Telecomm info	Telephone number	E	To identify individual in support of a lawful investigation To facilitate electronic surveillance, if required	
40	Contact	Telecomm info	Extension	E	To identify individual in support of a lawful investigation To facilitate electronic surveillance, if required	
41	Contact	Telecomm info	File number	E	To identify individual in support of a lawful investigation To facilitate electronic surveillance, if required	Associated with object
42	Contact	Telecomm info	Base	E	To identify individual in support of a lawful investigation To facilitate electronic surveillance, if required To support a lawful investigation to locate a subject	Geographic base associated with telecomm object

	Category	Element	Sub-Element	Format	Purpose / Necessity	Notes
43	Contact	Telecomm info	Aliases associated with object	E	To identify individual in support of a lawful investigation To facilitate electronic surveillance, if required	
44	Contact	Telecomm info	Activity	E	To facilitate electronic surveillance, if required	Criminal activity associated with object
45	Contact	Telecomm info	Commodity	E	To identify individual in support of a lawful investigation To facilitate electronic surveillance, if required To identify type of illicit activity	Type of commodity associated with object
46	Investigation	Transport data	Commodity type	E	To identify individual in support of a lawful investigation To identify type of illicit activity	Commodity type person was transporting
47	Investigation	Transport data	Concealment method	E	To identify individual in support of a lawful investigation To identify new concealment techniques	
48	Investigation	Transport data	Departure date	E	To support a lawful investigation to locate a subject	
49	Investigation	Transport data	Arrival date	E	To support a lawful investigation to locate a subject	
50	Investigation	Transport data	Net worth	E	To support a lawful investigation as a reflection of subject's legitimate means of income	May be used as a comparison against individual's lifestyle and spending habits to indicate presence of illicit source of funds

	Category	Element	Sub-Element	Format	Purpose / Necessity	Notes
51	Investigation	Transport data	Val date	E	To support a lawful investigation to confirm identity locations of transportation vehicles.	Confirms ownership of transport vehicles.
52	Investigation	Transport data	Status	E	To support a lawful investigation to locate a subject	Present whereabouts / condition of the commodity
53	Investigation	Transport data	Stop location table	E	To support a lawful investigation to locate a subject To support a lawful investigation if another entity is involved in organized crime activity	All stops made by the transport carrying the commodity
54	Investigation	Transport data	Activity	E	To identify criminal activity in support of a lawful investigation	Description of criminal activity suspected or confirmed
55	Investigation	Transport data	Type of identification	E	To identify entity in support of a lawful investigation	Identifying numbers associated to the object
56	Investigation	Transport data	Transport method	E	To identify entity and mode used in support of a lawful investigation	
57	Investigation	Transport data	Commodity description	E	To identify concealment method of illicit goods	
58	Investigation	Vehicle data	VIN, PIN, HIN	E	To identify entity in support of a lawful investigation	

	Category	Element	Sub-Element	Format	Purpose / Necessity	Notes
59	Investigation	Vehicle data	Licences	E	To identify entity in support of a lawful investigation	
60	Investigation	Vehicle data	Make	E	To identify entity in support of a lawful investigation	
61	Investigation	Vehicle data	Model	E	To identify entity in support of a lawful investigation	e.g. Sports Utility Vehicle
62	Investigation	Vehicle data	Style	E	To identify entity in support of a lawful investigation	e.g.. 2 door
63	Investigation	Vehicle data	Year	E	To identify entity in support of a lawful investigation	
64	Investigation	Vehicle data	Issued	E	To identify entity in support of a lawful investigation	Location of registration
65	Investigation	Vehicle data	Colour	E	To identify entity in support of a lawful investigation	
66	Investigation	Vehicle data	Base	E	To locate individual in support of a lawful investigation	Where vehicle is operated
67	Investigation	Vehicle data	Net worth	E	To support a lawful investigation as a reflection of subject's legitimate means of income	May be used as a comparison against individual's lifestyle and spending habits to indicate presence of illicit source of funds
68	Investigation	Vehicle data	Val date	E	To support a lawful investigation as a	May be used as a comparison

	Category	Element	Sub-Element	Format	Purpose / Necessity	Notes
					reflection of subject's legitimate means of income To determine expiration of Net Worth data element authenticity	against individual's lifestyle and spending habits to indicate presence of illicit source of funds
69	Investigation	Vehicle data	License plate alias	E	To identify entity in support of a lawful investigation	Any other license plates associated with this vehicle
70	Investigation	Vehicle data	Activity	E	To identify involvement of entity in support of a lawful investigation	Criminal activity associated with this vehicle
71	Investigation	Vehicle data	Commodity	E	To identify involvement of entity in support of a lawful investigation	Article of commerce or item of business relating to a criminal interest
72	Investigation	Vehicle data	Alias Vehicle Name	E	To identify entity in support of a lawful investigation	Aircraft only
73	Investigation	Vehicle data	Length	E	To identify entity in support of a lawful investigation	Watercraft only
74	Investigation	Vehicle data	Beam	E	To identify entity in support of a lawful investigation	Watercraft only
75	Investigation	Vehicle data	Tonnage	E	To identify entity in support of a lawful investigation	Watercraft only
76	Investigation	File ref. documents		E	To provide context of previous actions in support an ongoing lawful investigation	
77	Investigation	File ref. documents		E	To provide context of previous actions in support an ongoing lawful investigation	

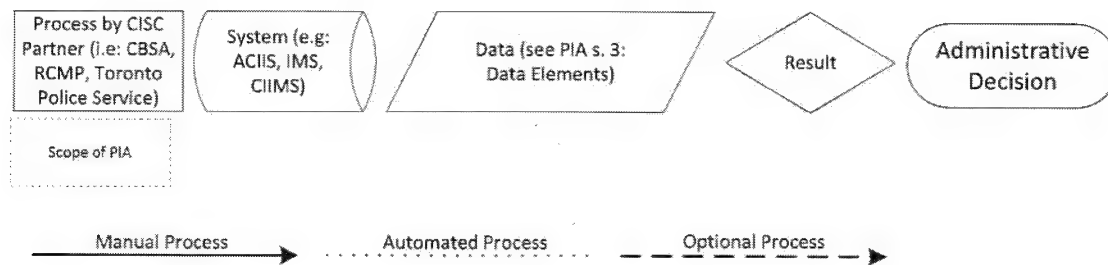
	Category	Element	Sub-Element	Format	Purpose / Necessity	Notes
78	Investigation	File ref. documents		E	To provide context of previous actions in support an ongoing lawful investigation	
79	Investigation	File ref. documents		E	To provide context of previous actions in support an ongoing lawful investigation	
80	Investigation	File ref. documents		E	To provide context of previous actions in support an ongoing lawful investigation	
81	Investigation	File ref. documents		E	To provide context of previous actions in support an ongoing lawful investigation	
82	Investigation	File ref. documents		E	To provide context of previous actions in support an ongoing lawful investigation	
83	Investigation	File ref. documents		E	To provide context of previous actions in support an ongoing lawful investigation	
84	Investigation	File ref. documents		E	To provide context of previous actions in support an ongoing lawful investigation	Including charts
85	Investigation	File ref. documents		E	To provide context of previous actions in support an ongoing lawful investigation	
86	Investigation	File ref. documents	Photographs	E	To identify an individual in support of an ongoing lawful investigation To provide context of previous actions in support an ongoing lawful investigation	
87	Investigation	File ref. documents	Images	E	To provide context of previous actions in support an ongoing lawful investigation	e.g. maps, handwritten notes, drawings
88	Investigation	File ref. documents	Spreadsheets	E	To provide context of previous actions in support an ongoing lawful investigation	

	Category	Element	Sub-Element	Format	Purpose / Necessity	Notes
89	Investigation	File ref. documents		E	To provide context of previous actions in support an ongoing lawful investigation	
90	Investigation	File ref. documents		E	This element may be collected by the CBSA from ACIIS if it supports a lawful investigation. Information collected will identify individuals involved in transnational serious and/or organized crime	
91	Investigation	File ref. documents	Other documents received	E	To provide context of previous actions in support an ongoing lawful investigation	Documents/information received from other police or non-police agencies.
92	Investigation	Misc. documents	Location, Organization / Business, Project, Association, Graphical object (link chart)	E	To provide context of previous actions in support an ongoing lawful investigation	

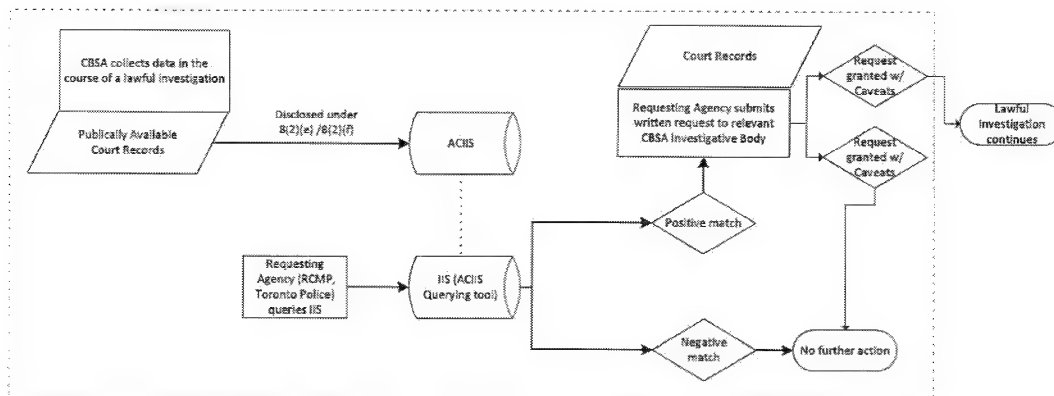
SECTION 4 - FLOW OF PERSONAL INFORMATION

4.1 Data Flow Model

Legend:



CBSA Disclosure to ACIIS



1. CBSA Criminal Investigations Division (CID) will collect court records related to investigations of serious or organized crime undertaken by the CBSA from publically available sources (see s. 3 1.CBSA Data to be uploaded to ACIIS). Records are stored in the Criminal Investigations Information Management System (CIIMS) within the relevant investigative case file. CID will review each record to ensure each court record directly relates to serious or organized crime before it is uploaded into ACIIS.

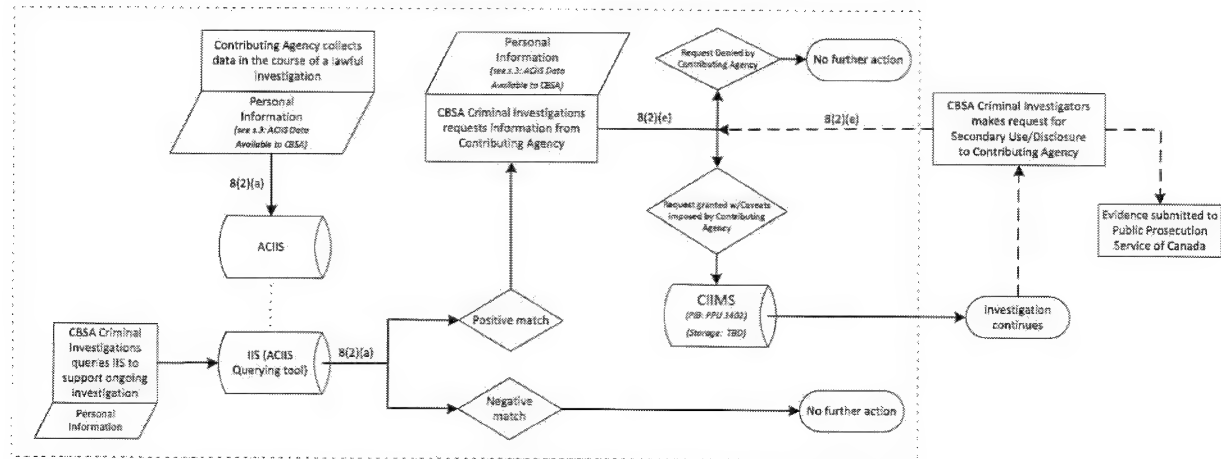
2. The Requesting Agency will query the IIS tool of the ACIIS system to obtain information to support a lawful investigation. The IIS query tool will retrieve any potential matches to the information queried by the Requesting Agency, prompting additional information requests to the CBSA for additional information.

3. If the match is negative, no further action will be taken.

4. If the match is positive, the originating body will make a written request to the relevant CBSA Investigative Body. The CBSA Investigative Body will evaluate the request and must impose the ACIIS Third Party rule caveat on the onward use or disclosure of the information. If the Requesting Agency is an Investigative Body listed in Schedule II of the *Privacy Regulations*, the CBSA will disclose this information under s. 8(2)(e) of the *Privacy Act*. If the Requesting Agency is a law enforcement agency at the Provincial level, this information will be disclosed under s. 8(2)(f) of the *Privacy Act* in accordance with the applicable MOU. Publicly available court records are excluded from s. 7 and s. 8 of the *Privacy Act* as a result of s. 69(2) of the *Privacy Act*. However, the CBSA has chosen to seek valid authorities under s. 8(2) in anticipation of expanding the list of data elements beyond publicly available court records.

5. The Requesting Agency will continue with their investigation. If the Requesting Agency requires additional information, they may choose to make a follow-up request through normal information sharing channels outside the scope of this PIA.

Criminal Investigations Division Collection, Use & Disclosure

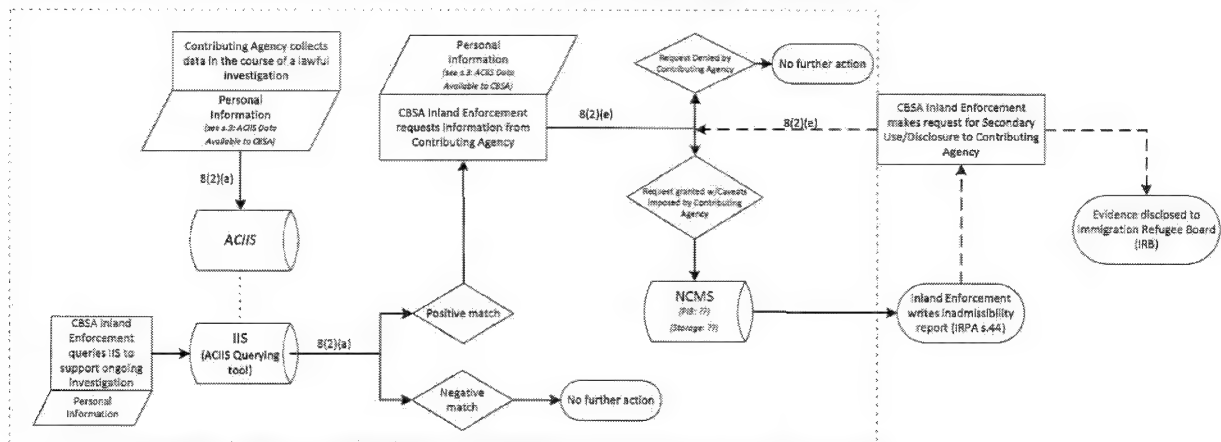


1. A Criminal Investigations Officer queries IIS to obtain information which supports prosecutions of a person(s) who is believed to have committed criminal offences against border legislation and may be involved in serious and/or organized crime activities.
2. If the IIS search results in a negative match, no further queries will be made in the system for this investigation.
3. If the IIS search results in a positive match for the person queried, the Criminal Investigations Officer does not use the data in any capacity. The officer collects the contributing police agency's contact details for the purposes of making a formal request to use the information in support of the CBSA investigation of a border crime.
4. A written request is submitted by the CBSA under section 8(2)(e) or (f) of the *Privacy Act* to the police agency. The request will detail the purpose for which the CBSA will use the information; authority to request and use the information; legislation(s) that will be enforced; and, notify the contributing police agency that the information may be shared internally within the CBSA.
 - a. If the contributing police agency denies the CBSA request for information, CBSA continues with the investigation.
 - b. If the contributing police agency approves CBSA request for use of the information, a written response is provided which may include additional caveats for the purpose and the scope for which the information can be used.
5. The Criminal Investigations Officer receives the information requested, in an electronic or paper format, which is entered into CIIMS. Caveats are also detailed advising that the information is "Third Party Information" and cannot be used for any other purpose other than the original intent for which it was disclosed to the CBSA.
6. The Criminal Investigations Officer uses the information to support CBSA investigation of a specific border related offence for prosecution purposes.

- a. The Criminal Investigations Division may make a subsequent request to the contributing police agency seeking additional details which may not have been provided in the original disclosure; or, request permission to use the information for a secondary purpose supporting the administration and enforcement of a border related crime.
7. The information may be disclosed to the Public Prosecutions Services of Canada to pursue prosecutions of a person(s) who commit criminal offences against border legislation. This type of disclosure would be outlined in the original written request.

Note: A written request must be made to the originating agency for each step in the investigative process. Requests must contain the specific details outlined in paragraph 8(2)(e) of the *Privacy Act*. Broadly worded requests with multiple uses are not permitted.

Inland Enforcement Operations Division Collection, Use and Disclosure



1. An Inland Enforcement Officer queries IIS to support an inadmissibility investigation of a foreign national or permanent resident of Canada for serious and/or organized crime concerns which are related to a border offence.
2. If the IIS search results in a negative match, no further queries made in the system for this investigation.

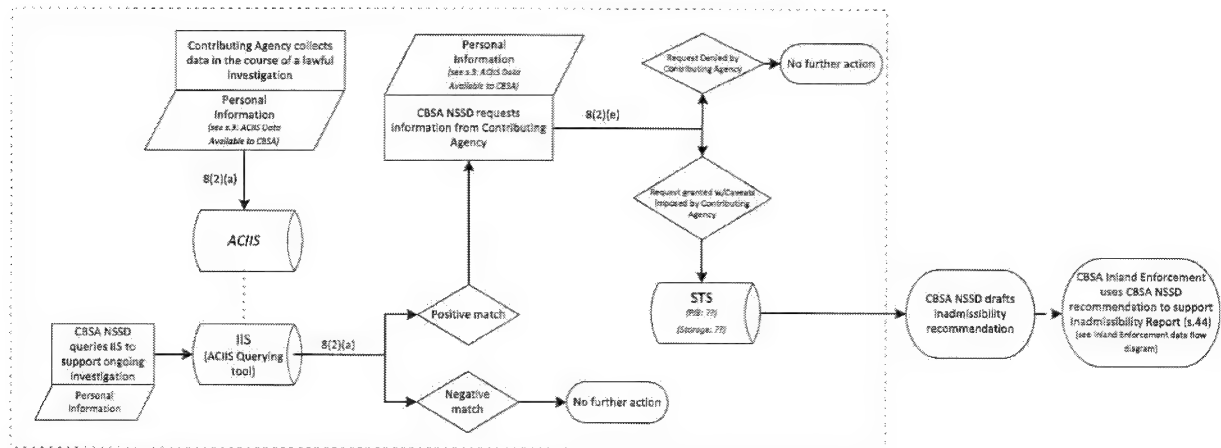
If an IIS search results in a positive match for the person queried, the Inland Enforcement Officer does not use the data in any capacity. The officer collects the contributing police agency's contact details for the purposes of making a formal request to use the information in support of the CBSA investigation of a border crime.

3. A written request is submitted by the CBSA under section 8(2)(e) or (f) of the *Privacy Act* to the police agency. The request will detail the purpose for which the CBSA will use the information, authority to request and use the information; legislation(s) that will be enforced; and notify the contributing police agency that the information may be shared with the Immigration and Refugee Board of Canada.
 - a. If the contributing police agency denies the CBSA request for information, CBSA continues with the investigation.
 - b. If the contributing police agency approves the CBSA request for use of the information, a written response is provided which may include additional caveats for the purpose and scope for which the information can be used.
4. The Inland Enforcement Officer receives the information requested in an electronic or paper format, which is entered into the NCMS system. Caveats are also detailed advising that the information is "Third Party Information" and cannot be used for any other purpose other than the original intent for which it was disclosed to the CBSA.
5. The Inland Enforcement Officer writes a report for inadmissibility purposes and processes the information provided by the contributing police agency supporting the CBSA investigation.

- a. The Inland Enforcement Officer may make a subsequent request to the contributing police agency seeking additional details which may not have been provided in the original disclosure; or, request permission to use the information for secondary purposes in support of the administration and enforcement of a border related crime.
6. Information is disclosed to the Immigration and Refugee Board of Canada in support of inadmissibility determination for removal purposes.

Note: A written request must be made to the originating agency for each step in the investigative process. Requests must contain the specific details outlined in paragraph 8(2)(e) of the *Privacy Act*. Broadly worded requests with multiple uses are not permitted.

National Security Screening Division (NSSD) Collection, Use & Disclosure



1. A National Security Screening Division Officer queries IIS to obtain supporting information for an inadmissibility determination of a refugee claimant, who is physically located in Canada, for serious and/or organized crime concerns.
2. If the IIS search results in a negative match, no further queries are made in the system for this investigation.

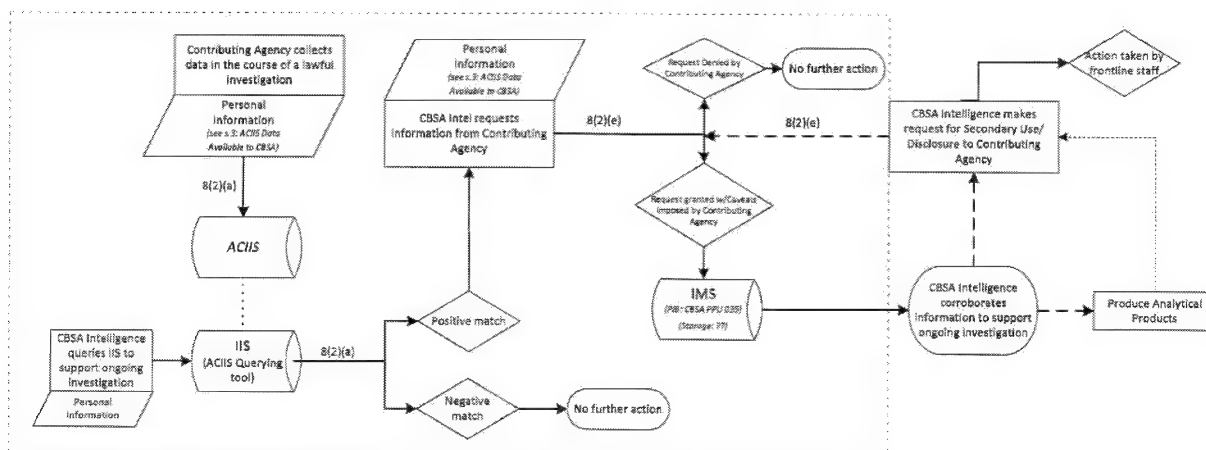
If the IIS search results is a positive match for person queried, the National Security Screening Division Officer does not use the data in any capacity. The officer collects the contributing police agency's contact details from the system for the purposes of making a formal request to use the information in support of the CBSA investigation of a border crime.

3. A written request is submitted by the CBSA under section 8(2)(e) or (f) of the *Privacy Act* to the police agency. The request will detail the purpose for which the CBSA will use the information; authority to request and use the information; legislation(s) that will be enforced; and notify the contributing police agency that the information may be shared internally within the CBSA, and with the Immigration and Refugee Board of Canada.
 - a. If the originating police agency denies the CBSA request for information, CBSA continues with the investigation.
 - b. If the originating police agency approves the CBSA request for use of the information, a written response is provided which may include additional caveats for purpose and scope for which the information can be used.
4. The National Security Screening Division Officer receives the information in an electronic or paper format which is entered into the Secure Tracking System (STS). Caveats are also detailed advising that the information is "Third Party Information" and cannot be used for any other purpose other than the original intent for which it was disclosed to the CBSA.
5. The National Security Screening Division Officer prepares an inadmissibility recommendation, supported by the information disclosed by the contributing police agency.

- a. The National Security Screening Division may make a subsequent request to the contributing police agency seeking additional details which may not have been provided in the original disclosure; or, request permission to use the information for secondary purposes in support of the administration and enforcement of a border related crime.
6. The inadmissibility recommendation is provided to the CBSA Inland Enforcement Operation for removal purposes (please see detail in *Inland Enforcement Operations* for detail on continued process).

Note: A written request must be made to the originating agency for each step in the investigative process. Requests must contain the specific details outlined in paragraph 8(2)(e) of the *Privacy Act*. Broadly worded requests with multiple uses are not permitted.

Intelligence Operations and Analysis Division Collection, Use & Disclosure



1. An Intelligence Operations and Analysis Division Officer will query IIS to develop intelligence leads to assist in the investigation of a border related crime linked to serious and/or organized crime through the production of analytical products (Annex E).
2. If the IIS search results is a negative match, no further queries are made in the system for this investigation.
3. If the IIS search results in a positive match for the entity queried, the Intelligence Operations and Analysis Division Officer does not use the data in any capacity. The officer collects the contributing police agency's contact details for the purposes of making a formal request to use the information in support of the CBSA investigation of a border crime.
4. A written request is submitted by the CBSA under section 8(2)(e) or (f) of the PA to the police agency; depending on whether the agency is a federal or provincial body. The request will detail the purpose for which the CBSA will use the information; authority to request and use the information; legislation(s) that will be enforced; and notify the contributing police agency that the information may be shared internally within the CBSA.
5. If the contributing police agency denies the CBSA request for information, CBSA continues with the investigation.
6. If the contributing police agency approves CBSA request for use of the information, a written response is provided which may include additional caveats for the purpose and scope for which the information can be used.
7. Intelligence Operations and Analysis Division Officer receives the information requested in an electronic or paper format, which is entered into the CBSA Intelligence Management System (IMS). Caveats are also detailed advising that the information is "Third Party Information" and cannot be used for any other purpose other than its original intent for which it was disclosed to the CBSA.

8. Intelligence Operations and Analysis Division Officer corroborates received data for links to serious and/or organized crime against CBSA data.
9. The Intelligence Operations and Analysis Division may make a subsequent request to the contributing police agency seeking additional details which may not have been provided in the original disclosure; or, request permission to use the information for secondary purposes in support of the administration and enforcement of a border related crime.
10. Analytical Products are disclosed internally amongst CBSA Intelligence and Enforcement Officials (e.g: BSOs, Targeting Officers, etc) to support enforcement efforts related to serious and organized crime. See Annex E for a List of Intelligence Analytical Products.

Note: A written request must be made to the originating agency for each step in the investigative process. Requests must contain the specific details outlined in paragraph 8(2)(e) of the *Privacy Act*. Broadly worded requests with multiple uses are not permitted.

4.2 Data Flow Model – Table

This table summarizes the flow of data illustrated in the data flow diagram above.

COLLECTION	SOURCE
Collection from the individual or a representative	The CBSA will collect and collate public court records of individuals or corporations brought to trial for customs or immigration infractions with a nexus to serious and/or organized crime.
Collection from a federal government institution	Under this framework CBSA investigative bodies will collect personal information from the RCMP's PIB CMP PPU 005 Operational Case Records.
Federal / Non-federal institutions	
400 federal, provincial, municipal law enforcement agencies accessing ACIIS through 10 provincial bureaux	RCMP, Canadian Forces Military Police, Ontario Provincial Police, Sûreté du Québec, Ottawa Police Services, Toronto Police Service, Vancouver Police Department, Service de police de la Ville de Montréal, etc.
Organization of a Foreign State	Category II membership may be granted to a foreign law enforcement or intelligence agency if, as determined by the respective Provincial Executive Committee, it is deemed to be in the best interests of the broader criminal intelligence community.
International Organization	International agencies such as Interpol are able to contribute to ACIIS as well as conduct queries with the assistance of a Provincial Bureau.
Private Sector	
Located in Canada and Canadian Owned	No private sector organizations contribute data to ACIIS.
Located in Canada and Foreign Owned	No private sector organizations contribute data to ACIIS.
Located abroad and Canadian Owned	No private sector organizations contribute data to ACIIS.
Located abroad and Foreign Owned	No private sector organizations contribute data to ACIIS.

4.3 Internal Use and Disclosure

USE / DISCLOSURE	Personal information bank
<p>Data collected by CBSA from ACIIS will be used by:</p> <ul style="list-style-type: none"> • Criminal Investigations Division, CBSA • Inland Enforcement Operations Division, CBSA • National Security Screening Division, CBSA • Intelligence Operations and Analysis Division, CBSA 	<ul style="list-style-type: none"> • CBSA PPU 035 • CBSA PPU 1402 • CBSA PPU 1403 <p>* A new Personal Information Bank will be created to cover the additional Investigative Body. This has been identified as a privacy risk in Section 6, below.</p>

4.4 External Use and Disclosure

Disclosed to the individual or a representative	NA
Disclosed to / used by federal government institutions	CISC federal member law enforcement agencies (RCMP, DND Military Police, Wildlife Service of Canada, etc.) <ul style="list-style-type: none"> • CMP PPU 005 Operational Case Records
Non-federal institutions and private sector	
Disclosed to / used by provincial governments	Provincial law enforcement partners (Ontario Provincial Police, Sûreté du Québec)
Disclosed to / used by municipal governments	Municipal law enforcement partners (Vancouver Police Department, Toronto Police Services, Service de police de la Ville de Montréal, Calgary Police Services, etc.)
Disclosed to aboriginal government / council	Aboriginal police services have Category 1 access to information contained in the ACIIS database
Disclosed to organizations of a foreign state	In accordance to ACIIS Policy and Regulations, Category II Membership may be granted to a foreign law enforcement or intelligence agency if, as determined by the respective Provincial Executive Committee, it is deemed to be in the best interest of the broader criminal intelligence community.
Disclosed to international organizations	In accordance to ACIIS Policy and Regulations, Category II Membership may be granted to a foreign law enforcement or intelligence agency if, as determined by the respective Provincial Executive Committee, it is deemed to be in the best interest of the broader criminal intelligence community.
Private Sector	
Located in Canada and Canadian Owned	No personal information will be disclosed to private sector organizations
Located in Canada and Foreign Owned	No personal information will be disclosed to private sector organizations
Located abroad and Canadian Owned	No personal information will be disclosed to private sector organizations
Located abroad and Foreign Owned	No personal information will be disclosed to private sector organizations

4.5 Retention / Storage

i. Records Collected by CBSA Investigative Bodies	
<p>Information collected by CBSA investigative bodies will be stored in the following CBSA systems:</p> <ul style="list-style-type: none"> • Criminal Intelligence Information Management System (CIIMS) <ul style="list-style-type: none"> ○ Criminal Investigations Division • National Case Management System (NCMS) <ul style="list-style-type: none"> ○ Inland Enforcement Division • Secure Tracking System (STS) <ul style="list-style-type: none"> ○ National Security Screening Division • Intelligence Management System (IMS) <ul style="list-style-type: none"> ○ Intelligence Operations Division <p>Records will be maintained in according with the associated PIB for each function. The CBSA has identified a privacy risk that some of these functions do not have a corresponding PIB. This privacy risk has been noted in Section 6 below.</p>	
ii. Records Disclosed by CBSA to CISC	
<p>Information disclosed by CBSA investigative bodies to CISC will be stored on a secure server at CISC headquarters in Ottawa and backed up on a regular basis (see CISC PIA for additional details).</p> <p>As per CISC policy, the CBSA is fully responsible for the accuracy and disposition of any records it uploads into the ACIIS. The CBSA will provide statistical data detailing seizures made by the Agency. When CBSA records have reached the end of their life cycle, the CBSA shall securely delete the records from all repositories (including ACIIS), in accordance with the record's disposition schedule, and the records will no longer be available to CISC policing partners. No information will be disclosed, used, retained or disposed of by organizations of a foreign state or international organizations.</p> <p>Record disposition schedules have not yet been assessed by CBSA Information Management. This privacy risk has been noted in Section 6 below.</p>	
Private Sector	
Records retained / stored by private sector organizations located in Canada and Canadian owned?	No information disclosed by CBSA investigative bodies will be retained / stored by private sector organizations.
Records retained / stored by private sector organizations located in Canada and foreign owned?	No information disclosed by CBSA investigative bodies will be retained / stored by private sector organizations.
Records retained / stored by private sector organizations located abroad and Canadian owned?	No information disclosed by CBSA investigative bodies will be retained / stored by private sector organizations.
Records retained / stored by private sector organizations located abroad and foreign owned?	No information disclosed by CBSA investigative bodies will be retained / stored by private sector organizations.

4.6 Other Considerations

In accordance with CISC national policy, the use of information uploaded to the ACIIS database and accessed by member agencies is governed by strict “Third Party” rules set out in ACIIS policy. These rules state, for example, that other agencies must not further disclose information, or use information for an administrative purpose without first contacting the originating agency. The CBSA Third Party Rule will be added to all documents uploaded to the ACIIS. The Third Party statement is noted below:

“This document is the property of the Canada Border Services Agency (CBSA) and should not be reclassified or disseminated without prior consent of the originator. The information must be stored, transmitted, and safeguarded in accordance with its classification level, as outlined in the Government Security Policy and the CBSA Security Policies. If access is requested under the Access to Information Act or the Privacy Act, no decision should be taken without prior consultation with the originator, as the information may be subject to exemptions. Requests for additional use should be forwarded to the Enforcement and Intelligence Operations Directorate, CBSA.”

SECTION 5 - PRIVACY COMPLIANCE ANALYSIS

5.1 Legal Authority for Collection of Personal Information

- 1.1 Has a legal authority been identified for the collection of personal information for this initiative?

Statutory reference: Section 4 of *Privacy Act* (*Section 4 has been interpreted to mean that a legal authority must be established for a collection of personal information, but section 4 does not provide legal authority for such a collection*).

Policy reference: Section 6.2.6 of *Directive on Privacy Practices*

Yes, legal authorities have been identified for the collection of personal information by the CBSA from public sources and from CISC's ACIIS database. Please see Section 1 (above).

- 1.2 Is the personal information collected directly related to an operating program or activity?

Yes. The personal information collected by the CBSA from the ACIIS system will be used by to support the Criminal Investigations, Inland Enforcement, and Intelligence programs.

5.2 Necessity to Collect Personal Information

- 2.1 Is each element and sub-element of personal information collected or to be collected necessary to administer the initiative?

Statutory reference: Section 4 of *Privacy Act*

Policy reference: Sections 6.1.1, 6.1.3, 6.1.4, 6.2.7 and 6.2.8 of *Directive on Privacy Practices*

Yes, each element and sub-element collected by the CBSA and uploaded to the CISC database is only information that is relevant to the case before the courts. Only information relevant to an ongoing investigation will be identified and retrieved by the CBSA from the ACIIS database.

- 2.2 ☒ Ensure that all personal information necessary to administer the initiative is listed in the relevant **PIB**.
- 2.3 ☒ Implement controls and procedures to ensure the CBSA does not collect more personal information than is necessary for the identified initiative and that a continuing need exists for that information or its collection.
- 2.4 Are secondary uses contemplated for the information collected?

No secondary uses are contemplated for the information collected by the CBSA from public court records or from the ACIIS database. Information collected from ACIIS cannot be used or stored within CBSA databases without prior written consent of the originator. No information may be used or disclosed for a secondary purpose without the consent of the originator of the information in accordance with the Third Party rule.

5.3 Authority for the Collection, Use or Disclosure of the Social Insurance Number

- 3.1 Is the collection of the Social Insurance Number (SIN) necessary to administer the initiative?

Statutory reference: Section 4 of *Privacy Act*

Policy reference: Section 6.2.13 of *Policy on Privacy Protection* and sections 6.1.1 and 6.2 to 6.4 of *Directive on Social Insurance Number*

Also see "Guidance for Preparing Information-Sharing agreements Involving Personal Information" and "Taking Privacy into Account Before making Contracting Decisions"

3.2	<input type="checkbox"/> Collection of the SIN must be in compliance with the <i>Directive on Social Insurance Number</i> (please check all appropriate boxes below):
3.3	<input type="checkbox"/> State legal authority for collecting the SIN:
No , the collection of the SIN is not necessary to administer the initiative.	
5.4 Direct Collection - Notification and Consent (as appropriate)	
4.1	Is personal information collected directly from the individual to whom it relates? Statutory reference: Sections 4 and 5 of <i>Privacy Act</i> Policy reference: Sections 6.1.1, 6.2.6 and 6.2.9 to 6.2.13 of <i>Directive on Privacy Practices</i> and section 6.1.2 and 6.4.1 of <i>Directive on Social Insurance Number</i> <i>CBSA Collection of Open Court Records:</i>
4.2	Yes , information used in judicial proceedings is collected directly from the individual. <i>CBSA Collection of ACIIS Data:</i>
4.3	No , the personal information collected by CBSA investigative bodies from the ACIIS database is not collected directly from the individual.
5.5 Indirect Collection - Consent or Authority under Sec. 10 of Privacy Regulations	
5.1	Is personal information collected indirectly from another source with the informed consent of the individual to whom it relates, or from a person authorized to act on behalf of the individual pursuant to section 10 of the <i>Privacy Regulations</i> ? Statutory reference: Sections 4 and 5 of <i>Privacy Act</i> and section 10 of <i>Privacy Regulations</i> Policy reference: Sections 6.1.1, 6.2.6 and 6.2.9 to 6.2.13 of <i>Directive on Privacy Practices</i> and sections 6.1.2 and 6.4.1 of the <i>Directive on Social Insurance Number</i>
5.2	No , the personal information collected by CBSA investigative bodies from the ACIIS database is not collected directly from the individual or their authorized representative under section 10 of the <i>Privacy Regulations</i> .
5.6 Indirect Collection - Without Notification and Consent	
6.1	Is personal information collected from another source without notice to or consent from the individual to whom the information relates? Statutory reference: Sections 4, 5, 7 and 8 of <i>Privacy Act</i> and section 10 of <i>Privacy Regulations</i> Policy reference: Sections 6.2.6 and 6.2.9 to 6.2.13 of <i>Directive on Privacy Practices</i> , section 6.2.15 of the <i>Policy on Privacy Protection</i> and sections 6.3.2 and 6.3.3 of <i>Directive on Privacy Impact Assessment</i>
Yes Where information is collected indirectly under any of the following circumstances without notice to, or consent from, the individual to whom it relates, please check the applicable boxes and explain as requested:	
<input checked="" type="checkbox"/> a) The collection is a result of a disclosure to the CBSA by the ACIIS contributor under subsection 8(2) of the <i>Privacy Act</i> . State the applicable paragraph(s) of subsection 8(2) and provide a brief explanation for each:	

6.2	<p>Details: Personal information is disclosed to the CBSA by the ACIS contributor for the purposes of lawful investigations into organized crime. The RCMP considers this a consistent use (s. 8(2)(a)) listed under RCMP PPU 005 (Operational Case Records). Further information may be requested for the purpose of investigating other serious offences to be disclosed by the originator under the investigative body designation provision (s. 8(2)(e) or the equivalent provision of the local data protection authority. In cases where there is an existing written agreement between the CBSA and the originating body, information will be disclosed under the terms of that agreement (s. 8(2)(f)).</p> <p><input checked="" type="checkbox"/> b) Direct notification of the individual might result in the collection of inaccurate information, or might defeat the purpose or prejudice the use for which the information is collected. Briefly explain why notice is not provided:</p> <p>Details: Notice that personal information may be collected indirectly from other sources <u>is not provided</u> to the subjects of CBSA investigations. A lawful investigation may be jeopardized if the investigators were required to notify subjects because they would take further steps to obscure their activities or cease their activities altogether.</p>
	<p><input checked="" type="checkbox"/> if any of the circumstances in a) b) or c) is applicable, ensure that it is reflected in the relevant PIB.</p>
5.7 Retention and Disposal of Personal Information	
7.1	<p>Has Library and Archives Canada approved a records retention and disposal schedule that applies to the personal information?</p>
	<p>Statutory reference: Section 12 of <i>Library and Archives Canada Act</i>, sections 6, 10 and 11 of <i>Privacy Act</i> and section 4 of <i>Privacy Regulations</i></p>
	<p>Policy reference: Sections 6.1.3, 6.2.11 to 6.2.13 and 6.2.23 of <i>Directive on Privacy Practices</i></p>
	<p>Yes</p>
	<p><input checked="" type="checkbox"/> Identify the Record Disposition Authority (RDA) and describe the retention and disposal schedule:</p> <p>Details: The RDA number is 2015/008. According to the Subject File Classification System for Criminal Investigations, most CIIMS records are retained for 7 years, and then deleted or transferred to Library and Archives Canada if they have enduring archival value. However, leads and referrals within CIIMS are retained for 10 years.</p>
7.2	<p><input checked="" type="checkbox"/> Implement controls and procedures to ensure that personal information used to make a decision that directly affects an individual will be retained for a minimum of two years after the last administrative action or, where a request for access to the information has been received, until such time as the individual has had the opportunity to exercise all his/her rights under the Act.</p>
7.3	<p><input checked="" type="checkbox"/> If the CBSA intends to dispose of personal information that has been used for an administrative purpose prior to the expiration of the two-year minimum retention standard established by the <i>Privacy Regulations</i>, it will obtain in writing the consent of the individual to whom the information relates before doing so.</p>
7.4	<p><input checked="" type="checkbox"/> The CBSA will cite the RDA number, the retention period and the disposition standards for the personal information in the relevant PIB.</p>
5.8 Accuracy of Personal Information	
8.1	<p>Will measures be adopted to ensure that personal information used by the CBSA for an administrative purpose is as accurate, up-to-date and complete as possible?</p>

<p>Statutory reference: Sections 6, 10 and 11 of <i>Privacy Act</i> and sections 10 and 11 of <i>Privacy Regulations</i></p> <p>Policy reference: Sections 6.1.1 and 6.2.9 to 6.2.16 of <i>Directive on Privacy Practices</i></p>	
<p>Yes</p>	
8.2	<p>Please check any of the following measures that will be adopted to ensure accuracy of the personal information and provide details as requested:</p>
8.2.1	<p><input checked="" type="checkbox"/> A data-matching process will be used to verify the accuracy of personal information against a “reliable source” (within or outside the CBSA) where this is authorized, or where consent was obtained.</p> <p>Details: The defendant’s name, addresses and other identifying information contained in the public court record are carefully compared with identifiers in the CBSA investigation file prior to upload into ACIS.</p>
8.2.2	<p><input checked="" type="checkbox"/> In cases where direct collection or consent is not feasible, the CBSA will obtain information from trusted sources (public or private) and verify accuracy against existing personal information before use.</p> <p>Details: ACIS has well-established standards and practices to ensure the accuracy, validity and relevance of data uploaded by contributing agencies. Each contributing agency is responsible for the data that they input. Reports are provided to ensure that records are validated at periodic intervals. Each agency is subject to an independent audit by ACIS auditors.</p>
8.2.3	<p><input type="checkbox"/> Technological methods will be used to identify errors and discrepancies.</p>
8.3	<p><input checked="" type="checkbox"/> AND, if measures are adopted other than “<i>direct collection or validation with the individual or with a person authorized to act on behalf of the individual</i>”, the CBSA must implement appropriate controls and procedures to ensure that:</p> <ul style="list-style-type: none"> a) the technique(s) and the specific source(s) used to validate or update the personal information are documented; b) individuals are given the opportunity, whenever possible, to request correction of any inaccurate personal information before the information is used in a decision-making process that affects them; c) personal information can only be modified or corrected by those within the CBSA who have the authority to do so; d) when personal information is corrected or annotated, the record of personal information indicates the date of the last correction or annotation and the source of the information used to make the correction or annotation; and d) when personal information is corrected or annotated, other authorized holders of the information are notified about the correction or annotation and that all copies of the information in the possession of the CBSA are corrected / annotated.
8.4	<p><input type="checkbox"/> AND, if appropriate, ensure that the “Privacy Notice” or “Consent Statement” and the relevant PIB are amended to identify the data-matching activity including the source(s).</p>
<p>5.9 Use of Personal Information</p>	
9.1	<p>Will the personal information collected for the initiative be used solely for the original purpose for which it was obtained or compiled, a use consistent with that purpose, or a purpose for which the information was disclosed to the institution pursuant to subsection 8(2) of the <i>Privacy Act</i>?</p>

Statutory reference: Sections 5 and 7 to 11 of *Privacy Act*

Policy reference: Sections 6.1.1, 6.1.9, 6.2.9 to 6.2.13 and 6.2.17 of *Directive on Privacy Practices*, section 6.2.15 of *Policy on Privacy Protection* and Section IV of Appendix C of *Directive on Privacy Impact Assessment*

Yes

- 9.2 ☒ Implement controls and procedures to ensure that access to the personal information for such purposes will be limited to authorized individuals who need to know the information to perform their official duties.

Details: Use of information collected from the ACIS is limited to the purpose for which it was disclosed, in accordance with s. 7(b) of the *Privacy Act*. Access to publically available court records uploaded to the ACIS database will be limited to individuals in Category 1, 2, and 2.a police agencies undertaking lawful investigations, as per CISC policy. However, publically available court records are excluded from the use (s.7) and disclosure (s.8) sections of the *Privacy Act* under s. 69(2). Access to ACIS data will be limited to investigators within the CBSA's four designated investigative bodies who have a "need to know" to further a lawful investigation.

- 9.3 ☒ A "Data Flow Diagram" and "Data Flow Table" are included (see "Section 4 – Flow of Personal Information") identifying the areas, groups and individuals (e.g., the positions) within the CBSA who have a need-to-know to access to or handle the personal information, including their geographical location and where the personal information will be stored or retained.

- 9.4 ☒ Information may be used for a non-administrative purpose, such as research, statistical, audit and evaluation purposes. This has been reflected in the associated PIBs, and the CBSA will adhere to the requirements and principles in the **CBSA Privacy Protocol For Non-Administrative Purposes** (2012), in accordance with section 6.2.15 of the *Policy on Privacy Protection* to address any impact that such non-administrative uses may have on privacy.

5.10 Disclosures Directly Related to the Administration of the Initiative

- 10.1 Will personal information be disclosed for purposes directly related to the administration of the initiative? (This includes, for example, disclosures to other programs within the CBSA, other federal institutions, other governments, international organizations, private sector organizations or individuals.)

Statutory reference: Sections 5 and 8 to 11 of *Privacy Act*.

Policy reference: Sections 6.2.10, 6.2.11 and 6.2.13 of *Policy on Privacy Protection*, sections 6.2.1 to 6.2.3 of *Directive on Social Insurance Number*, sections 6.1.9, 6.2.9 to 6.2.13 and 6.2.15 to 6.2.20 of *Directive on Privacy Practices* and section IV of Appendix "C" of *Directive on Privacy Impact Assessment*

Also see "Guidance for Preparing Information-Sharing agreements Involving Personal Information" and "Taking Privacy into Account Before making Contracting Decisions"

Yes

- 10.2 Please check all applicable boxes below and, for each disclosure, identify the name of the organization or third party to which personal information will be disclosed. If it is disclosed within the CBSA, please identify the branch and the initiative.

- 10.1.1 ☒ Within the CBSA for another program or activity

Details: Four investigative bodies related to a lawful investigations related to serious and organized crime.

- 10.1.2 ☒ Other federal government institutions

Details: CISC federal member law enforcement agencies (RCMP, DND Military Police, Wildlife Service of Canada, etc.)	
10.1.3 <input checked="" type="checkbox"/>	Provincial, territorial or municipal governments institutions CISC provincial, territorial and municipal member law enforcement agencies (Ontario Provincial Police, Vancouver Police Department, RCMP Contract Policing, etc.)
10.1.4 <input type="checkbox"/>	Foreign government institutions and entities thereof Details: No information will be disclosed to foreign governments or entities as part of the administration of this program.
10.1.5 <input checked="" type="checkbox"/>	International organizations Details: Information may be disclosed to international ACIIS partners including Interpol.
10.2 <input checked="" type="checkbox"/>	AND, ensure that: <ul style="list-style-type: none"> a) any such disclosure is made in compliance with section 8 of the <i>Privacy Act</i>, which allows disclosures of personal information with consent of the individual to whom the information relates (subsection 8(1)) or without consent in certain and limited circumstances pursuant to subsection 8(2) of the Act; b) only personal information elements that are necessary for the intended purpose are disclosed; c) the organization or third party receiving the personal information is authorized to do so; d) administrative, physical and technical safeguards appropriate to the sensitivity of the information will be applied to protect the information during and after its transmission (see Question 15); e) the organization or third party to which the personal information will be disclosed for the administration of the initiative are identified in the "Consistent Use" section in the relevant PIB in <i>CBSA Info Source</i>, including the specific purpose of the disclosure; f) the "Privacy Notice" or "Consent Statement" describes any disclosures of information and, g) the "Data Flow Diagram" or "Data Flow Tables" completed in "Section 4 – Flow of Personal Information" of the CBSA PIA include details on the disclosed personal information.
10.3 <input type="checkbox"/>	AND, any disclosure of personal information to another federal institution or outside the Government of Canada is governed by a formal agreement or arrangement (e.g., a Memorandum of Understanding, an accord, a contractual arrangement, etc.) to ensure that appropriate privacy protection clauses are included, and, where applicable, include provisions for inter-jurisdictional or trans-border flows of personal information. Such clauses must cover the following topics: <ul style="list-style-type: none"> a) Control over personal information, where appropriate. b) Limitations on the collection, retention, use and disclosure of personal information. c) Measures (administrative, technical and physical) to protect the integrity and confidentiality of personal information. d) Measures governing the disposition of the personal information, where relevant e) Measures to ensure or verify that the personal information is only used for the purposes related to the agreement, arrangement or contract. f) Obligations are to be extended to other parties such as subcontractors. Details: CBSA-CISC Memorandum of Understanding only governs the relationship between the two agencies and does not govern the sharing of information between partner agencies. Instead, a combination of consistent use (8(2)(a) of the <i>Privacy Act</i>), law enforcement assistance (8(2)(e)) of the <i>Privacy Act</i> , and MOUs with each province (8(2)(f)) of the <i>Privacy Act</i> will be used.

5.11 Accounting For New Uses or Disclosures Not Reported in CBSA Info Source

11.1 Will controls and procedures be implemented to account for any new use or disclosure of the personal information that is not included in the relevant **PIB** published in CBSA Info Source?

Statutory reference: Sections 7 to 11 of *Privacy Act* and section 4 of *Privacy Regulations*

Policy reference: Sections 6.1.9 and 6.2.2 of *Directive on Privacy Practices*

Yes

- 11.2 ☒ Appropriate controls and procedures have been or will be implemented to ensure that:
- a) the ATI and Privacy Director or the appropriate delegate is notified about any new use or disclosure of personal information that is not reflected in the **PIB** description published in *CBSA Info Source*;
 - b) the consent of the individual to whom the information relates is obtained in writing, as appropriate, prior to any new use of the information for an administrative purpose that is not reflected in the relevant **PIB** published in *CBSA Info Source*, unless the new use is considered to be consistent with the purpose for which the personal information was obtained or compiled and the Privacy Commissioner is notified, by the CBSA ATI and Privacy Director, forthwith regarding the new consistent use;
 - c) except as permitted under subsection 8(2) of the *Privacy Act*, any disclosure of personal information for a purpose that is not reflected in the relevant **PIB** published in *CBSA Info Source* will only be made with the consent of the individual to whom the information relates;
 - d) a record is kept for any new use or disclosure of personal information not described in the relevant **PIB** published in *CBSA Info Source*, and that this record is stored with the personal information to which it relates and retained for a minimum period of two years following such a use or disclosure. The record of use or disclosure will include the name and title of the person authorizing the use or disclosure; the name of the institution, person, organization or body receiving the information; a description of the use or purpose of disclosure; a copy of the information disclosed, or a description in sufficient detail to allow a determination of exactly what information was used or disclosed;
 - e) if the information is disclosed to a federal investigative body under paragraph 8(2)(e) of the *Privacy Act*, the record of disclosure will be kept in a separate **PIB** for a period of two years where it will be available to the Privacy Commissioner for review upon request; (e.g., *Standard PIB "Disclosure to Investigative Bodies" PSE 913*)
 - f) the Privacy Commissioner is notified, by the CBSA ATI and Privacy Director, forthwith, as required under subsection 9(4) of the Act, of any new use or disclosure that is consistent with the purpose for which the information was obtained or compiled, but which is not reflected in the relevant **PIB** published in *CBSA Info Source*;
 - g) the relevant **PIB** is amended in time for the next edition of *CBSA Info Source* to include any new use(s) or disclosure(s) that are consistent with the purpose for which the information was obtained or compiled, as well as any routine use(s) or disclosure(s) that do not fall within the categories of purpose of collection or consistent use; and
 - h) the Privacy Commissioner is notified, by the ATI and Privacy Director, prior to or forthwith, as required under subsection 8(5) of the Act, about any disclosures made or to be made in the public interest or in the interest of the individual to whom the information relates.

5.12 Safeguards - Statement of Sensitivity

- 12.1 Has a Statement of Sensitivity (SoS) or similar analysis been completed to assess the degree of sensitivity of the personal information to be collected and retained for the initiative? (Input to this section should be coordinated with and reviewed by the CBSA – IT - Security Directorate)

Statutory reference: Sections 7 and 8 of *Privacy Act*.

Policy reference: Appendix C of *Directive on Privacy Impact Assessment* and sections 6.2.17 to 6.2.21 of *Directive on Privacy Practices*, *Policy on Government Security*, *Operational Security Standard: Management of Information Technology Security (MITS)*

Yes

- 12.1 ☒ The information contained in the SoS or similar analysis has been taken into account when assessing the level of risks to privacy in "Section 2 - Risk Area Identification and Categorization" of the CBSA PIA.

5.13 Safeguards - Threat and Risk Assessment

- 13.1 Has a Threat and Risk Assessment (TRA) or a similar security assessment been completed for the initiative? (Input to this section must be coordinated with and reviewed by CBSA – IT - Security Directorate)

Statutory reference: Sections 7 and 8 of *Privacy Act*.

Policy reference: Appendix C of *Directive on Privacy Impact Assessment* and sections 6.2.17 to 6.2.21 of *Directive on Privacy Practices*, *Policy on Government Security*, *Operational Security Standard: Management of Information Technology Security (MITS)*

No

- 13.1 ☒ Reference the title of the TRA or other security assessment in "Section 6 – Supplementary Documents List" and provide a brief synopsis of the assessment in the space below:

Details: TRAs for source systems have not been completed. This risk has been identified in Section 6, below.

- 13.2 ☐ AND, obtain assurances from the officials responsible for the initiative that the measures recommended in the assessment have been implemented to ensure the confidentiality, availability and integrity of the personal information.
- 13.3 ☐ AND, ensure that any residual risks to personal information are known and accepted by the executive or senior official responsible for the initiative and the Head or delegated authority for the *Privacy Act*. (ATI and Privacy Director)

5.14 Safeguards - Administrative, Physical and Technical

- 14.1 Please identify below any administrative, physical and technical safeguards in place, or to be implemented, for this initiative to ensure the confidentiality, availability and integrity of the personal information.

Statutory reference: Sections 7 and 8 of *Privacy Act*

Policy reference: Appendix C of *Directive on Privacy Impact Assessment* and sections 6.2.17 to 6.2.21 of *Directive on Privacy Practices*, *Policy on Government Security*, *Operational Security Standard: Management of Information Technology Security (MITS)*

- 14.2 Administrative safeguards

☒ Internal security and privacy policies and procedures

	<input checked="" type="checkbox"/> Staff training on privacy and the protection of personal information <input checked="" type="checkbox"/> Screening and security checks of employees <input checked="" type="checkbox"/> Appropriate security levels for employees who will have access to personal information <input checked="" type="checkbox"/> Contingency plans and documented procedures in place to identify and respond to security and privacy breaches, and to communicate security violations to the data subject, law enforcement authorities and relevant program managers <input checked="" type="checkbox"/> Regular monitoring of users' security practices <input checked="" type="checkbox"/> Methods to ensure that only authorized personnel who need to know have access to personal information
14.2	Physical safeguards <input checked="" type="checkbox"/> Restricted access areas <input checked="" type="checkbox"/> Security guards <input checked="" type="checkbox"/> Identification badges are worn by staff at all times <input checked="" type="checkbox"/> After hours alarms and monitoring systems <input checked="" type="checkbox"/> Locked filing cabinets <input type="checkbox"/> Combination locks <input type="checkbox"/> Safes <input type="checkbox"/> Cipher locks (opened by programmable keypad) <input checked="" type="checkbox"/> Key cards <input type="checkbox"/> Video surveillance (closed-circuit television) <input checked="" type="checkbox"/> Secured server locations <input checked="" type="checkbox"/> Backups secured off-site <input type="checkbox"/> Other
14.3	Technical safeguards <input checked="" type="checkbox"/> Role-based user authorization and authentication <input type="checkbox"/> Biometrics <input checked="" type="checkbox"/> Passwords (minimum of 6 characters long, include alpha and numeric characters) <input checked="" type="checkbox"/> Passwords are changed by users every 90 days and recently used passwords cannot be re-used) <input checked="" type="checkbox"/> Password protected screensavers <input checked="" type="checkbox"/> Session-time out security (automatically locks an account after a session has been idle for a specified amount of time) <input checked="" type="checkbox"/> Firewalls <input checked="" type="checkbox"/> Intrusion Detection System (IDS) <input checked="" type="checkbox"/> Virtual Private Network (VPN) <input checked="" type="checkbox"/> Encryption of sensitive information <input checked="" type="checkbox"/> Government of Canada Public Key Infrastructure Certificates (PKI) <input checked="" type="checkbox"/> External Certificate Authority (CA) <input checked="" type="checkbox"/> Audit trails <input type="checkbox"/> Other
<p>Details: TRAs have not been completed for associated CBSA systems. This has been identified as a privacy risk in section 6, below.</p>	

5.15 Technology and Privacy - Tracking Technologies	
15.1	<p>Will the information system(s) used to deliver the initiative employ cookies or other tracking technologies to collect personal information about users and their transactions</p> <p>Statutory reference: Sections 4 to 10 of the <i>Privacy Act</i> and section 4 of <i>Privacy Regulations</i> Policy reference: Subsections 6.1.1, 6.1.3, 6.1.9, 6.2.9 to 6.2.13, 6.2.17 and 6.2.23 of <i>Directive on Privacy Practices</i></p> <p>No <input checked="" type="checkbox"/> Tracking technologies are not used to collect personal information about users.</p>
5.16 Technology and Privacy - Surveillance or Monitoring	
16.1	<p>Will the new or modified initiative result in new or increased surveillance or monitoring of a targeted population?</p> <p>Statutory reference: Sections 4 to 10 of <i>Privacy Act</i>, section 4 of <i>Privacy Regulations</i> and section 8 of the <i>Charter of Rights and Freedoms</i> Policy reference: Subsections 6.1.1, 6.1.9, 6.2.9 to 6.2.13 and 6.2.17 of <i>Directive on Privacy Practices</i></p> <p><input checked="" type="checkbox"/> Yes, the new or modified initiative will result in new or increased surveillance or monitoring of a targeted population.</p>
5.17 Considerations Related to Compliance, Regulatory Investigation, Enforcement	
17.1	<p>Does the initiative involve compliance/regulatory investigation or law enforcement, surveillance or intelligence gathering that targets specific individuals against whom penalties, criminal charges or sanctions may be applicable?</p> <p>Statutory reference: Sections 4 to 10 of <i>Privacy Act</i>, section 4 of <i>Privacy Regulations</i> and section 8 of the <i>Charter of Rights and Freedoms</i> Policy reference: Subsections 6.1.1, 6.1.9, 6.2.9 to 6.2.13 and 6.2.17 of <i>Directive on Privacy Practices</i></p> <p>Yes</p>
17.2	<p><input checked="" type="checkbox"/> Consult with your legal advisors to determine whether or not the compliance/regulatory investigation or law enforcement activities raise any issues relating to the <i>Charter of Rights and Freedoms</i>, the <i>Privacy Act</i> or other applicable acts.</p>
17.3	<p><input checked="" type="checkbox"/> AND, identify the legislative authority and the specific regulatory or law enforcement purpose involved: Details: Purpose of collection is to support lawful investigation into serious and organized crime.</p>
17.4	<p><input type="checkbox"/> AND, if the legislative authority differs from the legal authority for the initiative, ensure it is adequately reflected in the response to Question 1 of "Section 5 – Privacy Compliance Analysis" and in "Section 1 – Overview and PIA Initiation" of the CBSA PIA.</p>
17.5	<p><input checked="" type="checkbox"/> AND, any personal information collected or created as a result of such regulatory or criminal enforcement, surveillance or intelligence gathering initiative is described in the relevant PIB and in "Section 3 – Analysis of Personal Information Elements" of the CBSA PIA.</p>
17.6	<p><input type="checkbox"/> AND, the collection or use of personal information through these compliance / regulatory investigation or enforcement activities is adequately reflected in the "Privacy Notice", unless such notification might result in the collection of inaccurate information or defeat the purpose, or prejudice the use, for which the personal information is collected.</p>

☒ If notice about the compliance/regulatory investigation or law enforcement activities will not be provided.

Details: The CBSA does not seek consent for the collection and use of this information since this would defeat the purpose for the collection and compromise the investigation.

SECTION 6 – SUMMARY OF ANALYSIS AND RECOMMENDATIONS

The CISC-CBSA Information Sharing Framework PIA has identified a number of potential privacy risks above. The following section summarizes these privacy risks and provides recommendations for mitigation strategies for review by Program Areas, Senior Management, and the Chief Privacy Officer (CPO). The risks and recommendations will be incorporated into the CISC-CBSA Information Sharing Framework PIA Action Plan, found in Annex C.

1. National Security Screening Division is not reflected in *InfoSource*.

The National Security Screening Division (NSSD) is not currently covered by an existing Personal Information Bank (PIB). The CBSA is out of compliance with s. 10(1) of the *Access to Information Act* and this presents a privacy risk that individuals may not have the ability to access their personal information under the control of the CBSA.

2. Existing PIBs require updates to reflect the CBSA-CISC Information Sharing Framework.

The CBSA's *Info Source* contains a number of inaccurate or outdated references and must be updated to reflect the reality of each program or activity. The CBSA is out of compliance with s. 10(1) of the *Access to Information Act* and this presents a privacy risk that individuals may not have the ability to access their personal information under the control of the CBSA.

3. Threat Risk Assessments (TRA) have not yet been undertaken for all CBSA databases housing personal information collected from partner agencies.

The CBSA will store records received from ACIIS contributors in the Criminal Intelligence Information System (CIIMS), Intelligence Management System (IMS), Secure Tracking System (STS), and National Case Management System (NCMS). The CBSA inherited each of these legacy systems upon its creation and has not yet fully assessed the security safeguards of these systems through the Threat and Risk Assessment (TRA) methodology. However, the CBSA has assessed portions of these systems during the regular maintenance cycle and has endeavoured to ensure that all relevant safeguards have been put into place. The CBSA is out of compliance with the *Management of Information Technology Standard (MITS)* and this creates a privacy risk that personal information may not be fully safeguarded.

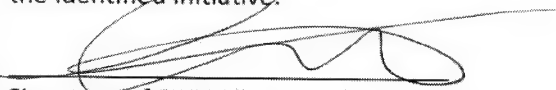
4. Record retention schedules for the CBSA databases housing personal information collected from partner agencies have not yet been applied.

The CBSA is currently reviewing its information management practices to ensure that information that is no longer necessary is destroyed. The first step of this process was obtaining a new Records Disposition Authority (RDA 2015-008) from Library and

Archives Canada. However, the retention schedule has not yet been fully operationalized within each of the CBSA databases described above. The CBSA is potentially out of compliance with its retention schedules which may create a risk that personal information may be retained longer than necessary thereby increasing the likelihood and/or severity of a privacy breach.

SECTION 8 - FORMAL APPROVAL

The following signature represents a commitment to comply with sections 4 to 8 of the *Privacy Act* and the related privacy policy requirements outlined in the CBSA PIA as they relate to the administration of the identified initiative.


Signature of CBSA Vice President lead for program or activity

MAR 23 2017

Date

Note: Responsibility for sections 4 to 8 of the *Privacy Act* rests with all employees of government institutions that handle personal information. Officials who manage such programs and activities are responsible for ensuring that such requirements are implemented as part of the administration of the program or activity.

The following signature represents a commitment by the Head of the institution or his/her delegate(s) who is responsible for establishing personal information banks in accordance with section 10 of the *Privacy Act*.


Signature of CBSA ATI and Privacy Director

APR 11 2017

Date

Note: Under the *Privacy Act*, the Head or his/her delegate(s) is responsible for complying with legal and relevant privacy policy requirements related to the approval and registration of personal information banks

SECTION 7 - SUPPLEMENTARY DOCUMENTS LIST

Document	Annex
<i>Privacy Compliance Checklist and Other Considerations</i>	A
<i>Office of the Privacy Commissioner Expectations</i>	B
<i>PIA Action Plan</i>	C
<i>CBSA Governance Model: Access and Use of the Automated Criminal Intelligence Information System</i>	D
<i>CBSA-CISC Statement of Cooperation</i>	E
<i>CISC Resolution 2014-04 CISC – CBSA Increased Information Sharing</i>	F
<i>CBSA-CISC Memorandum of Understanding (Draft)</i>	G

Annex A: Privacy Compliance Checklist and Other Considerations

Note: The table below must be used to keep an account of actions completed and to track outstanding actions required to achieve privacy compliance:

Privacy Compliance Analysis question #	Action required to support legal and policy compliance (cross reference to relevant question of <i>Section 5 – Privacy Compliance Analysis</i>)	Done	To be done	NA
1	Legal authority for the initiative has been established and is reflected in the relevant PIB.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
2	<p>a) The categories and elements of personal information to be collected for the new initiative have been carefully assessed based, for example, on the CBSA's experience gained with the administration of a similar initiative. The personal data collected will be limited to only that which is required.</p> <p>b) Categories and elements of personal information have been described in the relevant PIB for the initiative.</p> <p>c) Controls and procedures will be implemented to ensure the CBSA does not collect more personal information than necessary for the initiative and that a continuing need exists for the personal information and its collection.</p>	<input checked="" type="checkbox"/> <input type="checkbox"/> <input checked="" type="checkbox"/>	<input type="checkbox"/> <input checked="" type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
4 and 5	<p>a) All of the requisite "Privacy Notices" and "Consent Statements" that meet the requirements of sections 6.2.9 to 6.2.12 of the <i>Directive on Privacy Practices</i> have been drafted. (Texts of the notices and consent statements must be included as an annex.)</p> <p>b) Controls and procedures have been implemented to keep records of individual consents, and to ensure that persons acting on behalf of individuals who do not have the capacity to provide consent have the authority to do so under section 10 of the <i>Privacy Regulations</i>.</p>	<input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/>	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>
7	<p>a) A Records Disposal Authority (RDA) has been approved by Library and Archives Canada to authorize the disposal of the records containing personal information for the program.</p> <p>b) Controls and procedures have been implemented within the initiative and the CBSA ATI and Privacy Division to ensure that information that has been used for an administrative purpose will be kept for the minimum retention period established by the <i>Privacy Regulations</i>.</p> <p>c) Reference to the RDA, the retention period and the disposition standards for the program have been cited in the relevant PIB.</p>	<input checked="" type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>	<input type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

Privacy Compliance Analysis question #	Action required to support legal and policy compliance (cross reference to relevant question of <i>Section 5 – Privacy Compliance Analysis</i>)	Done	To be done	
8	Controls and procedures are in the process of being implemented to ensure that the personal information associated with the program is as accurate, complete and up-to-date as necessary.	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
Other Privacy Considerations related to specific principles that are not explored in the previous 17 sections: (these considerations should be explored in the Executive Summary)				
Openness	Describe how the results of any privacy impact assessment or audit will be made available to the public. The Executive Summary will be published on the external CBSA ATI and Privacy Division website at http://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/pia-efvp/atip-aiprp/pias-sefp-eng.html	<input type="checkbox"/>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Are policies and practices relating to the proposal's management and handling of personal information available to the public?	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
	Is there a communications plan to explain to the public how personal information will be managed and protected?	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
	Is there a clearly defined and easy process for individuals to access such information and/or communicate with appropriate individuals with respect to policies and practices relating to management and protection of personal information?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Where appropriate, will public consultation take place on the privacy implications of the proposal?	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Individual's Access To Personal Information	Is the system designed to ensure that an individual can have access to his/her personal information, including all other programs or applications that have received copies of the information? s. 12(1)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Are there documented procedures developed or planned on how to make privacy requests or requests for the correction of personal information? s. 12 (2)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Are individuals provided with access to their personal information in the official language of their choice? s. 17(2)	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	If appropriate, are individuals provided with access to their	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

Privacy Compliance Analysis question #	Action required to support legal and policy compliance (cross reference to relevant question of <i>Section 5 – Privacy Compliance Analysis</i>)	Done	To be done	NA
	personal information in an alternative format? s. 17(3)			
Challenging Compliance	Are the complaint procedures for the proposed program or service consistent with legislated requirements? s. 29-35	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	To improve information management practices and standards, has a procedure been established to log and periodically review the nature, frequency and resolution of complaints?	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>
	Are there oversight and review mechanisms implemented or available to ensure accountability?	<input checked="" type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
	Have oversight agencies, including the Office of the Privacy Commissioner, issued reports or opinions on issues that would be relevant to the proposal?	<input type="checkbox"/>	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Annex B: Office of the Privacy Commissioner Expectations

In their March 2011 document, *Expectations: A Guide for Submitting Privacy Impact Assessments to the Office of the Privacy Commissioner of Canada*, the Office of the Privacy Commissioner (OPC) has expressed the importance of analysing the risks of the project, program or initiative against the ten universal privacy and fair information practice principles of the Canadian Standards Association Model Code for the Protection of Personal Information.

The most relevant demonstration of the privacy risk and compliance analysis is the action plan. The OPC has said the following in their **Expectations** guide with respect to the action plan:

Once privacy risks and their proposed mitigating measures have been identified, we expect to see an Action Plan drawn up by the institution, indicating a specific time frame for remedying or mitigating the risks that have been identified, and if possible, naming a specific person or staff position accountable for taking action.

The action plan must list all privacy risks and compliance issues identified in the PIA and supplementary documentation. All risks and issues must be organized by the 10 universal privacy principles.

All recommendations and proposed mitigation strategies must also be described in the action plan. Identify the responsible program area and the timeline for completion or implementation of the strategy. The ATI and Privacy Division will provide programs with an action plan template to be addressed near the end of the PIA process.

The expectations of the OPC for each privacy principles are included below for your reference.

Accountability

Under this principle the OPC would expect to see documentation of an administrative structure for privacy, including input from legal services, access to information and privacy and information technology branches within an institution, with defined processes for determining when new projects require PIAs, for carrying them out, implementing mitigating measures and auditing for assurance of compliance. We expect PIA reports to be signed off at the appropriate level, and that training in privacy issues and procedures has been documented and is refreshed with employees regularly; and that privacy protective language is included in all contracts with third parties handling personal information in accordance with TBS guidance documents and internationally accepted best practices; and that regularly scheduled privacy compliance audits will be undertaken and the findings acted upon.

Identifying Purposes

The *Privacy Act* restricts federal government institutions to the collection of personal information that relates directly to an operating initiative of the institution, so we would expect to see a clear description of the program and why each piece of information is needed; a description of the legislative authority for the collection; a clear listing of all the data elements collected; copies of any relevant documents such as application forms identifying the purpose

for the collection or on-line notices of use; a copy of an up to date Personal Information Bank (PIB) description; a statement of any proposed new consistent use of information previously collected and a clear rationale as to how the use is reasonable and directly connected to the original collection – this may include an analysis of how an individual to whom it relates would reasonably expect it to be used for that purpose; a statement outlining any intended secondary uses of the information; whether the information is collected directly from the individual and if not, why; and a description of how personal information used for planning, forecasting or statistical purposes would be anonymized or de-linked from individual identifying information.

Consent

This is closely tied to the Identifying Purpose principle. Under this principle, OPC would expect to see a copy of notification language on forms or websites; a clear description of the purpose for collection; a rationale for not seeking consent, as is provided for in the *Privacy Act*; for web sites, a copy of the Privacy Notice Statement under which personal information is submitted to the institution.

Limiting Collection

Under this principle, OPC would expect to see a clear justification of the need for each data element collected, in keeping with the requirement of the *Privacy Act* that no personal information is to be collected by a government institution unless it relates directly to an operating initiative of the institution; an indication that a data minimization exercise has been undertaken to ensure that each data element is necessary and that this exercise will be refreshed regularly; and that information collected from another department for a secondary use will be purged of all but the essential data elements before use.

Limiting Use, Disclosure and Retention

Under this principle, OPC would expect to see a description of the specific uses and proposed disclosures of the information; a clear statement limiting the use of the information to the purposes identified; a clear retention policy and disposition schedule that is also noted in the PIB; a process for destruction of the information that is in keeping with the *Privacy Act* and Regulations; copies of MOUs or agreements with third parties to whom information is disclosed governing its use, retention and disclosure, and clauses with contractors or sub-processors of information indicating the originating institution has the right to audit for compliance with privacy provisions.

Accuracy

Under this principle, OPC would expect to see a description of the process used by entities to ensure accuracy, particularly when administrative decisions are made; a description of how changes to records are logged and monitored; a statement of whether automated decision-making based on risk profiles is being undertaken and how automated decisions are vetted for accuracy; an explanation of the processes open to individuals seeking to correct information; a description of the process by which second or third parties to whom information has been disclosed will be notified of changes and corrections to the record; and a description of how audit trails of records transactions are monitored and evaluated.

Safeguards

OPC would expect to see under this principle a description of the physical and electronic safeguards that are in place to protect information; a Threat & Risk Assessment (TRA) with emphasis on privacy risks and concerns and a discussion of how these concerns have been remedied or addressed; a notation that encryption is used for personal information both in transit and at rest; a description of how system logs of information transactions are monitored for inappropriate use, including viewing of the information; strong electronic access control, including controls on remote access, and the use of mobile devices; policies for the use of portable storage devices such as flash drives; a description of role-based access controls; and a description of the steps taken to ensure complete destruction of the information at the end of its life cycle.

Openness

Under this principle, OPC would expect to see a summary of the PIA written in plain, understandable language, posted on the institutional website in a manner accessible to the general public and containing a link to the relevant PIB description in CBSA Info Source; for particularly sensitive or privacy invasive programs we would expect to see the public communications plan described in the PIA, including a variety of methods such as posters, brochures and media announcements as well as detailed discussion of the PIA in the institution's Annual Report under the *Privacy Act*; a description of consultations with key stakeholders and the privacy risks or concerns raised should be readily available on the website; the name and contact information of an individual accountable for the handling of personal information should be easily obtained through the website or by calling the institution's main public number.

Individual Access

Under this principle, OPC would expect the PIA to include a description of any informal process the CBSA may have in place for access to and correction of personal information; an up to date and comprehensive description of information contained in the PIB corresponding to the initiative; a description of the process by which information in the hands of third parties is corrected following requests; a description of how the general public is made aware of these processes, for example, by a link and/or a toll-free number shown on the home page of the institutional website.

Challenging Compliance

OPC would expect to see the PIA address this principle by indicating clearly who is responsible for receiving and resolving privacy complaints; describing complaints that may have been received in any similar activity or pilot project and how they were handled; including privacy issues in project evaluations or feasibility reports; describing how and when compliance audits for privacy will be undertaken; including information on how to file a complaint with OPC under the *Privacy Act*; and reporting in some detail on specific and/or systemic privacy issues in its Annual Reports.

Annex C: PIA Action Plan

#	Risks	Proposed Mitigation Strategy	Expected Completion Date	OPI
1	The National Security Screening Division is not reflected in <i>InfoSource</i> .	The National Security Screening Division will work with ATIP in order to ensure that the program area continues to comply with privacy regulations.	On-going	Program Areas
2	Existing PIBs require updates to reflect the CBSA-CISC Information Sharing Framework.	<p>Proposed changes to the relevant PIBs have been noted in Section 1 of this PIA. The CBSA has committed with Treasury Board to a preliminary round of updates to <i>InfoSource</i> to be completed by June 2017. These updates include a reorganization to reflect the new Program Alignment Architecture of the Agency as well as updating references to both internal and external Divisions and departments.</p> <p>Phase 2 of the updates will address the gaps in the Agency's current PIA inventory and begin work on assessing legacy programs. There is no anticipated completion date for this Phase as it will be a continual process with the development of new programs.</p> <p>This PIA reflects the current Program Alignment Architecture.</p>	June, 2017	ATIP / Program Areas
3	Threat and Risk Assessments have not yet been undertaken for all CBSA databases housing personal information collected from partner agencies.	<p>An ongoing plan to identify and update requirements for TRA's on all legacy data repositories that do not have a defined decommissioning date has been undertaken by the CBSA.</p> <p>The Agency is currently in the process of approving Statements of Sensitivity for Intelligence Management System (IMS) and Criminal Intelligence Information Management System (CIIMS). Once approved, TRA's will be undertaken.</p> <p>A TRA was undertaken on NCMS by Immigration, Refugee and Citizenship Canada in 1998 prior to the creation of the CBSA.</p>	On-going	Program Area

#	Risks	Proposed Mitigation Strategy	Expected Completion Date	OPI
4	Record retention schedules for the CBSA databases described above have not yet been applied.	<p>As part of the exercise mentioned in #3, all current legacy systems without decommissioning date are being reviewed to ensure compliance with privacy, information management and IT management principles.</p> <p>During this review, purge dates will be examined and plans put in place to ensure data is stored and destroyed properly.</p>	On-going	Information Management / Program Areas

Annex D: CBSA Governance Model – Access and use of the Automated Criminal Intelligence Information System

PURPOSE

The purpose of the Governance Model document is to provide an overview for how the Canada Border Services Agency (CBSA) will support the Criminal Intelligence Services Canada (CISC) national strategy to combat serious and organized crime including the lawful authorities for the Agency to access; request and use the data contained in the Automated Criminal Intelligence Information System (ACIIS).

EXECUTIVE SUMMARY

The CBSA and CISC are significant contributors in the fight against serious and organized crime in Canada. On August 22, 2014, both agencies entered into a “Statement of Cooperation” and agreed to the “Adopted Resolution” confirming their commitment to enhance information sharing for the purposes of improving the detection and dismantling of serious and organized crime in Canada. CBSA access to ACIIS is facilitated by a Memorandum of Understanding (MOU) which defines the parties’ responsibilities regarding access and use of ACIIS and the framework for cooperation. ACIIS enhances the CBSA’s ability to identify persons and their networks involved in orchestrating and facilitating smuggling operations undermining the integrity of the border and threaten the security and prosperity of Canada. Obvious benefits of the CBSA partnership with the CISC are:

- **OFFICER SAFETY:** access to information previously unavailable warning of potentially dangerous encounters placing officers at risk;
- **INTELLIGENCE DEVELOPMENT:** increase inter-agency cooperation to identify modus operandi, trends, new and emerging threats, and additional leads supporting investigations; and,
- **DE-CONFLICTION:** advance knowledge of on-going investigations allowing greater opportunities to collaborate and leverage resources related to subjects of mutual interest.

Section 4 of the *Privacy Act* permits the CBSA to collect information contained in ACIIS for the purpose of carrying out a lawful investigation, if the request specifies the purpose and describes the information to be disclosed as it relates directly to an operating program or activity of the institution. Paragraph 8(2)(a) of the *Privacy Act* permits the CBSA to use information collected from the ACIIS for a purpose directly connected to serious and organized crime. CBSA purposes which directly involve law enforcement include: criminal enforcement of offences under various CBSA statutes; intelligence to identify serious border criminality; and inland immigration enforcement to detect and remove serious criminals from Canada. If additional information is required CBSA officers will seek written permission from the contributing law enforcement

agency to support an investigation of a border related crime(s) under paragraph 8(2)(e) of the *Privacy Act*.

CANADA BORDER SERVICES AGENCY RESPONSIBILITIES

The Agency is responsible for providing integrated border services that support national security and public safety priorities and facilitate the free flow of persons and goods, including animals and plants, that meet all requirements under the program legislation. The Agency's legislative, regulatory and partnership responsibilities include the following:

- administering legislation that governs the admissibility of people and goods, plants and animals into and out of Canada;
- detaining those people who may pose a threat to Canada;
- removing people who are inadmissible to Canada, including those involved in terrorism, organized crime, war crimes or crimes against humanity;
- interdicting illegal goods entering or leaving the country;
- protecting food safety, plant and animal health, and Canada's resource base;
- promoting Canadian business and economic benefits by administering trade legislation and trade agreements to meet Canada's international obligations;
- enforcing trade remedies that help protect Canadian industry from the injurious effects of dumped and subsidized imported goods;
- administering a fair and impartial redress mechanism;
- promoting Canadian interests in various international forums and with international organizations; and
- collecting applicable duties and taxes on imported goods.

CBSA Authority to Access and Use ACIIS Data

The lawful authorities for the CBSA's Investigative Body Designated (IBD) program areas to access and use ACIIS data in support of investigations enforcing legislation dealing with border related crime(s) are:

Privacy Act (Collection):

- Section 4 of the *Privacy Act* permits the collection of personal information by a government institution as long as it relates directly to an operating program or activity of the institution.

CBSA Act:

- Paragraph 5(1)(a) of the *CBSA Act*, the CBSA's mandate is to provide integrated border services that support national security and public safety priorities and facilitate the free flow of persons and goods that meet all requirements under its program legislation, by supporting the administration or enforcement of its program legislation.

Privacy Act (Use):

- Subsection 7(b) of the *Privacy Act* requires that "personal information" under the control of a government institution shall not...be used by the institution except...(b) for a

purpose for which the information may be disclosed to the institution under subsection 8(2) of the *Privacy Act*;

- Paragraph 8(2)(a) of the *Privacy Act* permits CBSA officials who have Investigative Body status to access personal information in ACIIS if its purpose is consistent with the reason why the information was initially collected;
- Paragraph 8(2)(e) of the *Privacy Act*, provides that a federal government institution may disclose information, upon request, to an investigative body where the information relates to a lawful investigation:

(Institutions with Investigative Body Designated (IBD) status are listed in Schedule II of the Privacy Regulations.)

Customs Act (IBD Designation):

- Subsection 2(1) of the *Customs Act* defines “officer” as a person employed in the administration and enforcement of the *Customs Act*, *Customs Tariff*, or *Special Import Measures Act*.

Immigration and Refugee Protection Act (IBD Designation):

- Subsection 6(1) of the *Immigration and Refugee Protection Act (IRPA)* provides the authority to designate officers to carry out any purpose of any provision of this Act.
- Pursuant to paragraph 3(1)(h), one of the objectives of the *IRPA* is to protect public health and safety and to maintain the security of Canadian society.

Privacy Regulations (IBD Designation) CBSA Programs Areas

1. Criminal Investigations Division (CID);
2. Inland Enforcement Operations (IEO);
3. National Security and Screening Division (NSSD)*;
4. Intelligence Operations and Analysis Division (IOAD); and,
5. National Targeting Centre Targeting Intelligence (NTC TI)*.

Within each IBD program area there will be a limited group of authorized personnel who will have the ability to conduct queries in ACIIS for intelligence and investigative purposes.

*(*It should be noted that Schedule II of the Privacy Regulations lists three divisions within the CBSA with IBD status. Due to re-engineering of the CBSA’s organizational structure there are now five IBD program areas. The Intelligence and Targeting Operations Division has been restructured into three separate IBD program areas comprising of Intelligence Operations and Analysis Division, National Targeting Centre and National Security Screening Division. Schedule II of the Privacy Regulations will require an update reflecting the five IBD program areas.)*

Types of Crimes:

The CBSA has access to unique information collected during the processing of persons and goods arriving or departing from Canada. Information pertaining to persons involved in a serious and organized crime can be shared with law enforcement partner agencies to assist an ongoing investigation. Examples of the types of criminal activities an organized crime group may be involved are: drug smuggling, human trafficking and money laundering which are indictable offences. An organized crime group is made up of three or more persons working in collaboration to facilitate a criminal activity from which they gain a personal benefit. CBSA information analyzed in conjunction with ACIIS data may assist to develop additional leads into a border related crime or a police investigation for organized crime activity.

CRIMINAL INTELLIGENCE SERVICE CANADA MANDATE

The mandate of the CISC is to lead the strategic and operational intelligence effort to combat organized crime and serious crime across Canada and help ensure the timely production and exchange of criminal information and intelligence among the law enforcement community, in support of the Canadian Law Enforcement Strategy to combat organized crime.

Another core mandate of the CISC is to provide comprehensive, timely assessments of criminal organizations and their activities with the goal of providing actionable intelligence aimed at more effectively controlling, reducing and preventing organized and serious crime in all communities across Canada. The CISC employs an intelligence-led approach to operations which serves to assist in the development and implementation of effective public policy, crime reduction and prevention strategies.

Automated Criminal Intelligence Information System (ACIIS)

ACIIS is the Canadian law enforcement community's national database containing criminal information and intelligence on organized and serious crime. Information contained within ACIIS is used in the production of the National Threat Assessment (NTA) that enhances the ability of law enforcement and government to develop strategies and policies to deal with organized and serious crime. ACIIS has become the information sharing tool used by the Canadian Integrated Response to Organized Crime (CIROC) for operationalizing National Targeting Enforcement Priorities (NTEPs) and the NTA.

ACIIS Data

In general terms, ACIIS contains data on criminals or suspected criminals and businesses or organizations if they are involved in organized crime, involved in serious crime that may affect more than one jurisdiction, or involved in specific activity as acknowledged and identified by the Director General of CISC.

THIRD PARTY RULE AND THE CONSISTENT USE REQUIREMENT

The CBSA will request permission, in writing, from the contributing law enforcement agency to use the data contained in ACIIS to investigate and enforce a border related crime. Paragraph 8(2)(a) of the *Privacy Act* and the application of the third party rule ensure that the consistent use elements are identified and articulated by the CBSA in all requests seeking permission to use ACIIS data. All requests made by the CBSA will include:

- the information the CBSA is seeking;
- authority to request and use information;
- legislation(s) that the information requested will assist to enforce; and,
- notify the contributing law enforcement agency if information will be shared outside the CBSA.

The mandate and responsibilities of all five IBD program areas are detailed in the proceeding sections. Examples demonstrating consistent use requirements, as set out in paragraphs 8(2)(a)&(e) of the *Privacy Act*, are also provided for reference purposes. The CBSA recognizes that having IBD status does not grant access to the ACIIS system; the CISC and Provincial Bureaus hold authority to approve or deny access of this system.

CBSA ACIIS REQUIREMENTS BY PROGRAM

Criminal Investigations Division:

The mandate of the Criminal Investigations Division (CID) is to support the CBSA's public safety and economic prosperity objectives by investigating and pursuing prosecution of those who commit criminal offences against specific border legislation.

CID investigates fraud and smuggling offences under the *Customs Act* and the *IRPA* as well as offences under or related to an additional 90 federal statutes that the CBSA administers. The CBSA's regional criminal investigators are responsible for operational activities including, but not limited to:

- investigating fraudulent activities related to the importation/exportation of goods and the movement of people;
- reviewing leads, researching, gathering evidence;
- executing search warrants;
- preparing and serving documents (corrective, civil, criminal);
- assisting foreign customs administrations with their investigation of customs offences via Customs Mutual Assistant Agreements, Mutual Legal Assistant Treaties; and,
- supporting criminal prosecutions (preparing Crown Briefs, recommending specific charges, assisting the Public Prosecution Service of Canada).

Regional investigators continue to investigate trans- jurisdictional smuggling operations planned by criminal organizations. These investigations often result in the identification of a person(s) and/or businesses operating across Canada; requiring greater coordination amongst federal, provincial and municipal law enforcement agencies. CID supports the access and use of ACIIS

data, the information contained in the system will assist in the identification and disruption of smuggling organizations. During the course of an investigation CID officers will:

- query ACIIS as per paragraph 8(2)(a) *Privacy Act*;
- contact the contributing law enforcement agency advising of CBSA interest and seek permission to use information contained in ACIIS as per subsection 7(b) and paragraph 8(2)(e) of the *Privacy Act*; and,
- use the information to enforce the *Customs Act* and the *IRPA*.

Data Elements:

“Vehicle Record Field” contains information valuable to CID investigators as the information can confirm licence plate information, make and model of vehicle(s) and associations to a person or business.

“Types of Individuals” field contains information investigators can use to develop additional investigative leads. The data may identify activities and associations unknown to the CBSA such as associations to a gang, suspect activities and linkages to organizations. Criminal investigators are required to attend interviews at ports of entry, at a public and private locations, execute warrants, interview and arrest and transport person(s) in the custody of the CBSA. Access to “types of individual data” will assist to anticipate and identify violent behaviours and those of associates that may be encountered in the dwelling during the course of the investigation; recognizing the importance of officer safety.

Further examples of ACIIS data elements supporting CID investigators are detailed in the Privacy Impact Assessment.

Inland Enforcement Operations:

The mandate of the CBSA Inland Enforcement Operations (IEO) is to enforce the regulatory provisions of the *IRPA* related to immigration investigations, hearings, detentions and removals of inadmissible persons in Canada. Inland enforcement officers support the objectives of IEO and enforce the regulatory provisions of *IRPA* by:

- identification of individuals inadmissible to Canada under the *IRPA*, including persons inadmissible due to serious and organized criminality;
- conduct interviews and prepare inadmissibility reports;
- issue removal orders;
- refer inadmissibility reports for review/decision to the Immigration and Refugee Board (IRB);
- arrest and detain inadmissible persons who are a flight risk;
- arrest and detain inadmissible persons who are or may be a danger to the public;
- issue Canada-wide immigration warrants for arrest and detention;

- investigate the whereabouts of absconders;
- arrange the removal of inadmissible persons; and,
- conduct escorted removals of individuals to their countries of origin.

IEO also holds responsibility for national operational planning and case management of irregular migrant arrivals. During these specific cases the IEO ensures the effected regional office(s) has access to all available information and resources to appropriately assess and make a determination for admissibility to Canada. Support and functional guidance is provided to the effected CBSA regional offices in making a determination for inadmissibility based on linkages to serious criminality, organized crime, war crimes/crimes against humanity and national security concerns.

The IEO supports the access and use of ACIIS data; information contained in the system will support the determination for admissibility purposes. The information will assist enforcement officers to locate individuals avoiding CBSA enforcement action and the subsequent removal process. Inland enforcement officers using ACIIS will:

- query ACIIS as per paragraph 8(2)(a) *Privacy Act*;
- contact the contributing law enforcement agency advising of CBSA interest and seek permission to use information contained in ACIIS as per subsection 7(b) and paragraph 8(2)(e) of the *Privacy Act*; and,
- use the information to enforce the *IRPA* and the regulations.

Data Elements:

“Person Record Field” contains information inland enforcement officers may use to support the removal of a person inadmissible to Canada. The data contained in the Person Record Field will assist officers to confirm the identity and any linkages to criminality, supporting the enforcement and subsequent removal of an individual for inadmissibility purposes.

“Telecommunications Record Field” contains data which may assist inland enforcement officers locate, detain and or arrest absconders from Canada. Access and use of this information will allow inland enforcement officers further opportunities to locate a person avoiding the removal process. Inland enforcement officers are required to assess risk to officer safety prior to any enforcement actions and during inland enforcement investigations. Access to ACIIS data may mitigate or notify CBSA officers of any safety concerns unknown to the CBSA.

Further examples of ACIIS data elements supporting IEO investigators are detailed in the Privacy Impact Assessment.

National Security Screening Division:

The National Security Screening Division (NSSD) of International Region, Operations Branch, is responsible for the screening of temporary and permanent residence applicants seeking entry to Canada as well as in-Canada refugee claimants. The NSSD is responsible for conducting *IRPA* screenings of persons for potential inadmissibility for organized crime, crimes against humanity and genocide, terrorism, espionage and subversion. To achieve these objectives, NSSD ensures the timely delivery of security screening products and services to clients both internal and external to the CBSA. Criminal organizations have become increasingly more sophisticated; operating beyond traditional borders and representing enforcement challenges to traditional law enforcement agencies. Only through collaborative efforts can law enforcement agencies effectively identify and enforce the operations of transnational and national criminal organizations targeting Canada.

Access to the ACIIS data will allow NSSD officers to conduct comprehensive and timely security screenings of refugee claimants physically located in Canada, with linkages to organized crime and represent a public safety concern. NSSD officers provide recommendation to CBSA enforcement officers of persons with linkages to serious and organized crime to be removed from Canada. NSSD officers using ACIIS will:

- query ACIIS as per paragraph 8(2)(a) *Privacy Act*;
- contact the contributing law enforcement agency advising of CBSA interest and seek permission to use information contained in ACIIS as per subsection 7(b) and paragraph 8(2)(e) of the *Privacy Act*; and,
- use the information to enforce the *IRPA* and the regulations.

Data Elements:

“Person Record Field” contains data which may assist to screen refugee claimants residing in Canada, for linkages to serious and organized crime activities. During the screening process, NSSD officers routinely encounter cases involving applicants suspected of supporting transnational criminal organizations

the applicant’s association to proceeds of crime activities or identifying linkages to organized crime supports NSSD officers recommendations into further investigations into the activities of the refugee claimant for linkages to organized crime which may result in the determination of inadmissibility.

Further examples of the ACIIS data elements supporting the NSSD officers are detailed in the Privacy Impact Assessment.

Intelligence Operations and Analysis Division:

The Intelligence Operations and Analysis Division (IOAD) holds responsibility for the production of operational, strategic and tactical intelligence for the purpose of strengthening the effectiveness, efficiency and the delivery of the integrated intelligence and enforcement priorities of the CBSA. The IOAD collects intelligence from multiple sources and performs analysis of the data for the purposes of production and the dissemination of strategic, operational and tactical intelligence products and services. Other key functions are:

- functional intelligence support;
- guidance to decision-makers for the purposes of proper risk management based on the current threat environment;
- timely distribution of intelligence products and delivery of services to internal and external stakeholders and clients.

Access to ACIIS will provide additional opportunities for IOAD analysts to collect data to identify the current threat environment and the development of mitigation strategies supporting border integrity. IOAD officers will use ACIIS data supporting CBSA regional intelligence offices and their operations through the development of intelligence products identifying the activities of national and transnational organizations. IOAD officers using ACIIS will:

- query ACIIS as per paragraph 8(2)(a) *Privacy Act*;
- contact the contributing law enforcement agency advising of CBSA interest and seek permission to use information contained in ACIIS as per subsection 7(b) and paragraph 8(2)(e) of the *Privacy Act*; and,
- use the information to enforce the *Customs Act* and the *IRPA*.

Data Elements:

“Person Record Field” contains data IOAD analysts may use to develop intelligence and leads identifying companies, vehicles and associates unknown to a law enforcement partner agency involved in an active investigation.

“Transportation Record Field” contains data that can be analysed and developed for the purposes of issuing lookouts on vehicles associated to human smuggling operations or the transportation of crime guns into Canada. The information collected by CBSA from border enforcement operations can be used to support multi-agency enforcement operations.

Further examples of the ACIIS data elements supporting the IOAD analysts are detailed in the Privacy Impact Assessment.

National Targeting Centre:

At this time, the CISC will not grant the National Targeting Centre (NTC) access to ACIIS. However, after the one year review the National Executive Committee may reassess the recommendation for possible inclusion of the NTC.

Annex E – CBSA – CISC Statement of Cooperation

Statement of Cooperation

Between

The Canada Border Services Agency

And

The Criminal Intelligence Service Canada

BACKGROUND:

The Canada Border Services Agency (CBSA) and the Criminal Intelligence Service Canada (CISC) are significant contributors in the fight against serious and organized crime in Canada.

In August 2013, the CISC National Executive Committee (NEC) mandated CISC to explore the current contribution of the CBSA to the Law Enforcement Community and identify solutions to increase information sharing between the two agencies.

In September 2013, the CBSA and the CISC established a Joint Working Group (JWG) to develop and implement a work plan to improve information sharing. Regular bi-weekly meetings have been held, issues identified, and progress made against them.

This Statement of Cooperation confirms our commitment concerning the conditions and procedures for continued cooperation in the development of enhanced information sharing mechanisms for the purposes of combatting serious and organized crime.

STATEMENT:

The purpose of this statement is to define the working partnership and the shared responsibilities between the CBSA and the CISC for the timely exchange of intelligence with the goal of identifying threats posed by serious and organized crime groups in Canada. This partnership will ultimately result

Page 1 of 4

in: increased information sharing; improved communication; and enhanced service delivery to all Canadians.

The CBSA and the CISC understand the overarching objective of their relationship is to facilitate the prevention, disruption and reduction of criminal activity. By doing so, law enforcement will strengthen the alignment between intelligence and operations, all in support of intelligence-led law enforcement.

MANDATES:

CBSA

The CBSA is responsible for providing integrated border services that support national security and public safety priorities and facilitate the free flow of persons and goods, including animals and plants that meet all requirements in the Agency's program legislation under the *Canada Border Services Agency Act* (CBSA Act).

The CBSA, under the authority of the CBSA Act and other legislation, delivers this mandate by:

- Enforcing the *Customs Act*, the *Immigration and Refugee Protection Act* and border related legislation at all CBSA Ports of Entry (POE), including alternative report locations;
- Interdicting illegal goods entering or leaving Canada at designated CBSA POE;
- Conducting inland immigration investigations and intelligence gathering to identify and remove people who are inadmissible to Canada, including those involved in terrorism, organized crime, war crimes or crimes against humanity;
- Investigating and gathering intelligence (at POEs and inland) on unlawful activities related to the importation/exportation of goods and the cross-border movement of people; and,
- Providing support internationally through the CBSA Liaison Officer network.

CISC

The mandate of the CISC is to lead the strategic and operational intelligence effort to combat organized crime and serious crime across Canada and help ensure the timely production and exchange of criminal information and intelligence among the law enforcement community, in support of the Canadian Law Enforcement Strategy to combat organized crime.

Another core mandate of the CISC is to provide comprehensive, timely assessments of criminal organizations and their activities with the goal of providing actionable intelligence aimed at more effectively controlling, reducing and preventing organized and serious crime in all communities across Canada. The CISC employs an intelligence-led approach to operations which serves to assist in the development and implementation of effective public policy, crime reduction and prevention strategies.

PARTNERSHIPS AND CONSULTATIVE PROCESS:

The CBSA and the CISC will continue to host, on a rotational basis, working group and sub-working group sessions. Consultations will be inclusive, requiring agreement from all affected participants. The working group will provide oversight and strategic guidance, representing their respective agencies but working as a group to reach integrated goals. The working group will continue to develop a high level work plan which serves as a roadmap to strengthen the CBSA-CISC relationship while monitoring the progress of the work plan and providing regular updates to respective senior management on key activities and initiatives.

To enhance our collective efforts to combat the threats of serious and organized crime, the CBSA and CISC will have the shared responsibility of:

- Exploring opportunities within lawful authority to provide or expand direct or indirect access to enforcement and intelligence systems within the scope of their respective areas of responsibility.
- Developing a policy framework, within the applicable legal framework, supporting a broader and lawful sharing of criminal investigations and intelligence information.
- Developing a Concept of Operations for greater information sharing and interoperability

INFORMATION SHARING:

It is the intention of the CBSA and the CISC to begin the negotiation of a Memorandum of Understanding which will list the types of information approved for release to the respective agencies in an automated format. This MOU will be developed in tandem with expanded or new systems accesses ensuring policy and operational synergies with the technical solutions.

Information shared under this SOC will be limited to statistical data which doesn't directly or indirectly identify any person, information sharing business requirements, enforcement and intelligence system technical specifications, best practices and information sharing policies, protocols and concepts of operations in support of the developing MOU.

OVERSIGHT AND CONFLICT RESOLUTION:

To ensure a consistent and transparent application of the shared responsibilities, the CBSA – Director General, Enforcement and Intelligence and the CISC Director General, Criminal Intelligence, their alternates or representatives, will establish joint protocols and a consultative process for the exchange

of information, the development of business requirements, and other management issues related to the application of this statement.

Ongoing oversight will be provided by the responsible CBSA and the CISC program managers. Where there are differences in determining the appropriate divisions of responsibility and resolution cannot be reached at the program manager level, the matter will be referred up the chain of command within each organization's Headquarters. Frequent interactions are vital to ensure open dialogue.

CONCLUSION:

The CBSA and CISC will continue to collaborate effectively to strengthen border security and enhance our collective efforts to combat serious and organized crime and threats to the security of Canada. Through mutual respect and transparent dialogue, our goal is to deepen the CBSA and CISC relationship.



Luc Portefance

President
 Canada Border Services Agency

2014-08-22
 Date



Bob Paulson
 Chair CISC National Executive Committee

Commissioner
 Royal Canadian Mounted Police

2014-08-22
 Date

Annex F – Resolution CISC 2014-04 CISC-CBSA Increased Information Sharing



Criminal Intelligence
 Service Canada

Service canadien de
 renseignements criminels



Adopted by NEC on August 22, 2014.

RESOLUTION CISC/SCRC 2014-04

CISC – CBSA Increased Information Sharing

Adoptées par le CEN en date du 22 août 2014.

RÉSOLUTION CISC/SCRC n° 2014-

**04 Amélioration de l'échange d'information
 entre le SCRC et l'ASFC**

WHEREAS the CISC National Executive Committee is guided by the principles of integration and being intelligence-led; and

WHEREAS ACIS is the national common platform for the sharing of information and intelligence between Canadian police services; and

WHEREAS the Canada Border Services Agency (CBSA) requests further access to the ACIS data bank and proposes to consider further contribution to the intelligence community; and

WHEREAS CBSA authority is provided under specific federal legislation (e.g. the CBSA Act, the Immigration and Refugee Protection Act, the Customs Act, etc.), it is understood that information sharing by CBSA is guided by such legislation; and

WHEREAS in 2013 the National Executive Committee mandated the creation of a working group composed of CISC and CBSA to consider the present level of contribution by the CBSA in an effort to define and increase where possible their levels of contribution; and

WHEREAS the working group identified significant levels of contribution in multiple local regional and national law enforcement venues; and

WHEREAS the working group explored and defined legislative limits and opportunities to increase information sharing between the CBSA and the greater law enforcement community; and

WHEREAS the working group identified links between the requested information and the investigative mandate of the requestor as defined in the consistent use principles; and

WHEREAS we, the National Executive Committee, recognized that the sharing of information is guided by the Privacy Legislation, Federal Legislation and Provincial Laws.

ATTENDU QUE le Comité exécutif national du SCRC est guidé par les principes de l'intégration et de la répression criminelle axée sur le renseignement;

ATTENDU QUE le Système automatisé de renseignements criminels (SARC) est la plate-forme commune d'échange d'information et de renseignements entre les services de police canadiens;

ATTENDU QUE l'Agence des services frontaliers du Canada (ASFC) demande un accès élargi à la banque de données du SARC et propose d'accroître son apport à la collectivité du renseignement;

ATTENDU QUE le pouvoir de l'ASFC lui est conféré par une législation fédérale précise (p.ex. Loi sur l'ASFC, Loi sur l'immigration et la protection des réfugiés, Loi sur les douanes) et que l'échange d'information par l'ASFC est régie par cette législation;

ATTENDU QUE le Comité exécutif national a prescrit, en 2013, la création d'un groupe de travail composé d'employés du SCRC et de l'ASFC pour étudier et déterminer le niveau de contribution actuel de l'ASFC en vue de l'augmenter, si possible;

ATTENDU QUE le groupe de travail a déterminé que l'ASFC apportait une contribution importante sous plusieurs aspects de l'application de la loi à l'échelle régionale et nationale;

ATTENDU QUE le groupe de travail a défini, selon la législation, les limites et les possibilités liées à l'amélioration de l'échange d'information entre l'ASFC et l'ensemble de la collectivité d'application de la loi;

ATTENDU QUE le groupe de travail a établi des liens entre l'information demandée et les mandats d'enquête des demandeurs, conformément à des principes d'utilisation uniformes;

ATTENDU QUE le Comité exécutif national a reconnu la mise en commun de l'information est guidée par la législation sur la protection des renseignements personnels ainsi que la législation fédérale et les lois provinciales;



Criminal Intelligence
Service Canada

Service canadien de
renseignements criminels



We, the CISC National Executive Committee, endorse:

1. The present efforts to facilitate access to intelligence through the Public Safety Portal (PSP) to data published within existing records management systems in accordance with the Governance Based Access Control and consistent with the Privacy Impact Assessment;
2. To create a national service desk at the CISC office supported and staffed by a CBSA officer to facilitate information sharing requests by both agencies;
3. The continued efforts of the working group to increase information sharing by facilitating limited access to ACIS information through the RPP/PSP portal to members of the three investigative bodies of CBSA (Inland Enforcement Division, Intelligence and Targeting Operations Directorate, Criminal Investigations Division);
4. To continue the efforts to find longer more sustainable and broader sharing opportunities between CBSA and the greater law enforcement community in keeping with Privacy Legislation and Provincial and Federal legislative parameters that guide our investigative mandates.

Le Comité exécutif national appuie :

1. les mesures prises actuellement pour faciliter l'accès aux renseignements par le Portail de la sécurité publique (PSP) et l'accès aux données publiées dans le système de gestion des dossiers, conformément au contrôle d'accès en fonction de la gouvernance et à l'évaluation des facteurs relatifs à la vie privée;
2. la création d'un service d'assistance national dans le bureau central du SCRC qui serait soutenu et pourvu en personnel par un agent de l'ASFC en vue de faciliter le traitement des demandes d'échange d'information des deux organismes;
3. les mesures prises par le groupe de travail pour améliorer la mise en commun de l'information en accordant un accès limité à l'information contenue dans le SARC par le Portail d'informations policières (PIP) et le PSP aux membres des trois organismes d'enquête de l'ASFC (Division de l'exécution de la loi dans les bureaux intérieurs, Direction des opérations relatives au renseignement et au ciblage, Division des enquêtes criminelles);
4. la poursuite de l'étude visant à trouver des options plus durables et plus vastes à long terme pour la mise en commun de l'information entre l'ASFC et la collectivité de l'application de la loi, conformément à la législation sur la protection des renseignements personnels et aux dispositions fédérales et provinciales régissant les mandats d'enquête.

Annex G – CBSA-CISC Memorandum of Understanding

Place Holder for MOU.

Use of Enhanced Driver's Licence and Enhanced Identification Card Information by the Canada Border Services Agency

Addendum to the Privacy Impact
Assessment (PIA) titled Enhanced Driver's
Licence and Enhanced Identification Card
Program - Use of EDL Data by the CBSA

Traveller Processing Enhancements Unit
Traveller Transformation – Land, Rail and Marine Division
Traveller Programs Directorate / Programs Branch

July 2017

Version Control

Version	Author	Action	Date
0.1	Yvonne Robinson	Creation of document includes Treasury Board Secretariat policy requirements (2010). Incorporates more detailed privacy analysis to reflect expectations of the Office of the Privacy Commissioner (2011). User friendly with examples and explanatory notes. Includes an Action Plan for implementing mitigating strategies.	Friday, March 13, 2015
0.2	Yvonne Robinson	Update document with initial program comments	April 8, 2015
0.3	Arleigh Romyn	Update document with comments from IT review	October 29, 2015
0.4	Arleigh Romyn	Further revisions to include RFID Processor	February 22, 2016
1.0	Arleigh Romyn	Update document with comments from manager review, general content review	April 19, 2016
1.1	Arleigh Romyn	Updates to reflect guidance from ATIP	June 8, 2016
1.2	Heather Vallier	Updated content referring to LSFD and edited additional content	August 8, 2016
1.3	Arleigh Romyn	Updates to reflect/address feedback	August 25, 2016
1.4	Arleigh Romyn	Finalized for Approvals	September 1, 2016
2.0	Arleigh Romyn	Approval Copy	September 8, 2016
2.1	Arleigh Romyn	All ATIP comments incorporated. Clean copy for Senior Management approvals	May 10, 2017
2.1	Arleigh Romyn	Further revisions requested by Director and discussed with ATIP analyst	June 12, 2017

PIA Participants

Name	Role	Contact Information
Maria Romeo	Director	Maria.Romeo@cbsa-asfc.gc.ca
Ron Warren	A/Manager	Ron.Warren@cbsa-asfc.gc.ca
Arleigh Romyn	Senior Program Advisor	Arleigh.Romyn@cbsa-asfc.gc.ca
Yvonne Robinson	Privacy Consultant	
Dan Proulx	ATIP Coordinator	Dan.Proulx@cbsa-asfc.gc.ca

Use of Enhanced Driver's Licence and Enhanced Identification Card Information by the Canada
Border Services Agency

PIA

Table of Contents

VERSION CONTROL	2
PIA PARTICIPANTS	2
EXECUTIVE SUMMARY	6
ABBREVIATIONS AND ACRONYMS	8
DEFINITIONS	11
SECTION 1 - OVERVIEW AND INITIATION	12
SECTION 2 - RISK AREA IDENTIFICATION AND CATEGORIZATION	17
Type of Program or Activity	17
Type of Personal Information Involved and Context	18
Program or Activity Partners and Private Sector Involvement	19
Duration of the Program or Activity	19
Program Population	20
Technology and Privacy	20
Personal Information Transmission	21
Risk Impact to the CBSA	23
Risk Impact to the Individual or Employee	23
SECTION 3 - ANALYSIS OF PERSONAL INFORMATION ELEMENTS	24
SECTION 4 - FLOW OF PERSONAL INFORMATION	26
4.1 Data Flow Model - Diagram	26
4.3 Internal Use and Disclosure	32
4.4 External Use and Disclosure	34
4.5 Retention / Storage	34
4.6 Other Possible Considerations	36
SECTION 5 - PRIVACY COMPLIANCE ANALYSIS	38
1. Legal Authority for Collection of Personal Information (if unsure, consult with Legal Services)	38
2. Necessity to Collect Personal Information	39
3. Authority for the Collection, Use or Disclosure of the Social Insurance Number	40
4. Direct Collection - Notification and Consent (as appropriate)	41
5. Indirect Collection - Consent or Authority under Sec. 10 of Privacy Regulations	42
6. Indirect Collection - Without Notification and Consent	43
7. Retention and Disposal of Personal Information	43
8. Accuracy of Personal Information	45
9. Use of Personal Information	46
10. Disclosures Directly Related to the Administration of the Program or Activity	47
11. Accounting For New Uses or Disclosures Not Reported in CBSA Info Source	49
12. Safeguards - Statement of Sensitivity	50
13. Safeguards - Threat and Risk Assessment	51
14. Safeguards - Administrative, Physical and Technical	51
15. Technology and Privacy - Tracking Technologies	53
16. Technology and Privacy - Surveillance or Monitoring	53
17. Considerations Related to Compliance, Regulatory Investigation, Enforcement ..	56

SECTION 6 - SUMMARY OF ANALYSIS AND RECOMMENDATIONS.....	58
SECTION 7 - SUPPLEMENTARY DOCUMENTS LIST	59
SECTION 8 - FORMAL APPROVAL	61
ANNEX A: PRIVACY COMPLIANCE CHECKLIST AND OTHER CONSIDERATIONS.....	61
ANNEX B: OFFICE OF THE PRIVACY COMMISSIONER EXPECTATIONS	64
ANNEX C: CATEGORIES OF PERSONAL INFORMATION	67

Privacy Impact Assessment Date / Version:	YYYY-MM-DD (Date sent to OPC)
Office of the Privacy Commissioner file #:	
Project Implementation Plan (if applicable)	2017-09-07
Federal Institution:	Canada Border Services Agency (CBSA)
Related Class of Record Number:	CBSA IST 004
Personal Information Bank:	CBSA PPU 061
Government Official Responsible for PIA:	Mr. Martin Bolduc, Vice President, Programs
Delegate for section 10 of the <i>Privacy Act</i> :	Mr. Dan Proulx, ATI and Privacy Director

EXECUTIVE SUMMARY

The Executive Summary will be published on the [CBSA ATI and Privacy Division website](#).

Enhanced Driver's Licence / Enhanced Identification Card

This Privacy Impact Assessment (PIA) is an addendum to the PIA submitted in December 2008 entitled *Enhanced Driver's Licence and Enhanced Identification Card Program – Use of EDL data by the CBSA*, which is a collaborative program between the Canada Border Services Agency (CBSA) and three participating provinces: Ontario, Manitoba and British Columbia. A fourth province, Quebec, also initially participated but discontinued the availability of a Quebec Enhanced Driver's Licence (EDL) to new applicants in October 2014. Quebec EDLs currently in circulation will remain active until they expire, and as such, are out of scope for this addendum. These provinces earlier agreed to make available enhanced documents (such as a Drivers Licence or an Identification Card) that meets the requirements of the Western Hemisphere Travel Initiative, allowing Canadian citizens to use the identification to facilitate land or water travel between Canada and the United States (U.S.).

Personal information is collected by the provinces and provided to the CBSA to enable query access by U.S. Customs and Border Protection in the event that a Canadian presents their card as identification at a land/water Port of Entry. Historically, the EDLs/ Enhanced Identification Cards (EICs) were only available for use to enter the U.S. The CBSA's Border Services Officers (BSO) did not have query access to the database to verify the validity of the documents, and accepting them as identification to confirm citizenship for re-entry was at the discretion of the BSO. The CBSA has undertaken the policy and technology work to permit BSOs to have access to the CBSA's EDL database and equipped select Ports of Entry with Radio Frequency Identification (RFID) abilities to read the card. Ports of Entry that are not RFID-enabled will still be able to scan/swipe the cards and access the CBSA database. It should be noted that CBSA BSOs have always had access to the Lost Stolen Fraudulent Document Database (LSFD) module within the Field Operations Support System (FOSS), which is now the Global Case Management System (GCMS).

It is expected that this information will become available to CBSA BSOs in October 2017.

Protecting your Personal Information

The following personal information elements are managed by the Traveller Programs – Program and Policy Management:

Transmitted by the province to the CBSA when the EDL / EIC is issued:

- Name (Given (First) Name and Surname (Last))
- Birth date
- Biographical Information (Gender)
- Identifying Numbers (Restriction and Endorsement Codes, Tag Identification Number (TID), Optical Character Recognition unique identifier (Encoded Document Number (EDN))
- Radio Frequency Identification (RFID) unique identifier (ID)
- Validity Dates (Issue and Expiry Dates)
- Visual Image of EDL holder
- Citizenship of Individual
- Licence/Card Status
- Issuing Country
- Issuing Jurisdiction (province)
- Document Type

Available on the card when used by the holder to cross at a land / water Port of Entry:

- Name
- Address
- Birth Date
- Driver Licence Number
- Driver Licence Class
- Validity Dates (Issue and Expiry Dates)
- Picture of Entitled Holder
- Biographical Information (Height, Weight, Eye Colour, Hair Colour, Gender)
- RFID chip (embedded)
- Citizenship (denoted by the "C")
- Signature of EDL holder
- Identifying Numbers (Restriction and Endorsement Codes, Tag Identification Number (TID), Optical Character Recognition unique identifier (Encoded Document Number (EDN))
- Radio Frequency Identification (RFID) unique identifier (ID)

There is no intention to change the elements of personal information to be collected, used or disclosed.

ABBREVIATIONS AND ACRONYMS

Note: Using the table format below, list any abbreviations and acronyms that are used in this report. Expand the list to include acronyms specific to the program or initiative, as necessary.

The following is a list of abbreviations and acronyms used in this report:

AFIS	Automated Fingerprint Identification System
ATIP	Access to Information and Privacy
BC	British Columbia
BCI	Border Crossing Information
BCI SORN	Border Crossing Information System of Records Notice
BSO	Border Services Officer
CBSA	Canada Border Services Agency
CPIC	Canadian Police Information Centre (CPIC)
CSQ	Client Status Query
EDL	Enhanced Driver's Licence (please note: the use of the acronym EDL in this document refers to both EDLs and EICs unless specified otherwise)
EDN	Encoded Document Number
EIC	Enhanced Identification Card
FOSS	Field Operations Support System
GOC	Government of Canada
GCMS	Global Case Management System
ID	Identification
IDS	Intrusion Detection System
IBAS	Interdiction and Border Alerting System
IBM	International Business Machines Corporation
IBQ	Integrated Border Query
ICBC	Insurance Corporation of British Columbia
ICES	Integrated Customs Enforcement System
IMS	Intelligence Management System
IPIL	Integrated Primary Inspection Line
IRPA	<i>Immigration and Refugee Protection Act</i>
ISA	Information Sharing Agreement

IT/IM	Information Technology/Information Management
LAN	Local Area Network
LSF	Lost/Stolen/Fraudulent
MOU	Memorandum of Understanding
MPI	Manitoba Public Insurance
MRZ	Machine Readable Zone
MTO	Ministry of Transportation Ontario
MWCS	Modern War Crimes System
NCIC	National Crime Information Center
NCMS	National Case Management System
OGD	Other Government Departments
OPC	Office of the Privacy Commissioner of Canada
ORS	Occurrence Reporting System
PA	<i>Privacy Act</i>
PAXIS	Passenger Information System
PH	Passage History Database
PI	Personal Information
PIA	Privacy Impact Assessment
PIB	Personal Information Bank
PKI	Public Key Infrastructure
POE	Port of Entry
RDA	Records Disposal Authority
RFID	Radio-Frequency Identification
SAAQ	Société de l'assurance automobile du Québec
SoS	Statement of Sensitivity
SP	Secondary Processing System
SSI	Support System for Intelligence
STS	Secure Tracking System
TBS	Treasury Board Secretariat
TID	Tag Identification number
TRA	Threat and Risk Assessment
TRCS	Telephone Reporting Centre System

Use of Enhanced Driver's Licence and Enhanced Identification Card Information by the Canada
 Border Services Agency

PIA

UCI	Unique Client Identifier
U.S. CBP	United States Customs and Border Protection
WHTI	Western Hemisphere Travel Initiative

DEFINITIONS

This section provides definitions of the terms frequently used in this report:

Action Plan	The Action Plan describes the steps that the Program will take to address risks that have been identified by ATI and Privacy Division, OPC and TBS.
Administrative Purpose	The <i>Privacy Act</i> defines an "administrative purpose" to be the use of an individual's personal information in a decision-making process that directly affects that individual.
Consistent use	A consistent use is a use that has a reasonable and direct connection to the original purpose(s) for which the information was obtained or compiled. This means that the original purpose and the proposed purpose are so closely related that the individual would expect that the information would be used for the consistent purpose, even if the use is not spelled out.
Data Matching	A comparison of personal data obtained from a variety of sources, including personal information banks, for the purpose of making decisions about the individuals to whom the data pertains. Data matching is a specialized activity involving the collection, use and disclosure of personal information that is subject to the various requirements of the <i>Privacy Act</i> .
Info Source	Is a series of annual Treasury Board Secretariat publications in which government institutions are required to describe their institutions, program responsibilities and information holdings, including PIBs and classes of personal information. The descriptions are to contain sufficient clarity and detail to facilitate the exercise of the right of access under the <i>Privacy Act</i> .
New Consistent Use	Is a consistent use that was not originally identified in the appropriate Personal Information Bank (PIB) description in the government institution's chapter in Info Source.
Personal Information	Information about an identifiable individual as defined in section 3 of the <i>Privacy Act</i> . This definition, although lengthy, is not exhaustive, as indicated by the introductory phrase, "including, without restricting the generality of the foregoing". Information that is not specifically mentioned in the list may still be included in the definition of personal information if it qualifies as "information about an identifiable individual".
Personal Information Bank	Is a description of personal information that is organized and retrievable by a person's name or by an identifying number, symbol or other particular assigned only to that person. The personal information described in the personal information bank has been used, is being used, or is available for an administrative purpose and is under the control of a government institution.
Privacy	The Office of the Privacy Commissioner of Canada describes "privacy" as "... the right to control access to one's person and information about one's self. The right to privacy means that individuals get to decide what and how much information to give up, to whom it is given, and for what uses."
Radio Frequency Identification	Radio-frequency identification (RFID) unique identifier (ID) is the wireless use of electromagnetic fields to transfer data, for the purposes of automatically identifying and tracking tags attached to objects. CBSA will implement "vicinity" RFID, allowing an RFID chip to be read within 3 – 5 metres of an RFID antenna.

SECTION 1 - OVERVIEW AND INITIATION

Report Objectives

This report is an addendum to the Privacy Impact Assessment (PIA) for the Enhanced Driver's Licence / Enhanced Identification Card Program of the Canada Border Services Agency (CBSA). The objectives of this PIA are:

- to review the business processes in order to identify the data flow of personal information;
- to analyze the collection, use, disclosure and retention of personal information;
- to determine if there are any associated privacy risks; and
- to provide recommendations on the mitigation or elimination of the risks.

The information presented in this report follows the Treasury Board of Canada Secretariat Privacy Impact Assessment policy and guidelines.

The purpose of a PIA process is to ensure that privacy is considered throughout the project development cycle. The results of a PIA are a documented guarantee that privacy issues have been identified and adequately addressed.

Government Institution: Canada Border Services Agency

Government Official Responsible for the Privacy Impact Assessment

Mr. Martin Bolduc
CBSA, Vice President, Programs

Head of the government institution / Delegate for section 10 of the *Privacy Act*

Mr. Dan Proulx
CBSA Access to Information and Privacy Director

Name of Program or Activity of the Government Institution:

Enhanced Driver's Licence/Enhanced Identification Card (EDL/EIC) Information

Description of Program or Activity:

Port of Entry Operations: Admissibility Determination: Highway Mode

Through the Admissibility Determination Program activity, the CBSA develops, maintains and administers the policies, regulations, procedures and partnerships that enable border services officers to intercept people and goods that are inadmissible to Canada and to process legitimate people and goods seeking entry into Canada within established service standards.

Description of the class of records associated with the program or activity:

Enhanced Driver's Licence/Enhanced Identification Card (EDL/EIC) Information

Description: Describes records related to the EDL/EIC Program, which is a voluntary program available to eligible Canadians who reside in a province or territory where the Program is offered by that Province or Territory. May include records identified in the electronic systems used to administer or manage the information including the Canada Border Services Agency (CBSA) EDL/EIC database and the CBSA Lost Stolen Fraudulent Document Database (LSFD), which is a module of the CBSA Interdiction and Border Alerting System (IBAS).

Class of Record Number: CBSA IST 004

- ☐ Proposal for a New Personal Information Bank
- ☒ Proposal to modify an existing Personal Information Bank - identify PIB registration number and current description:

(Modifications to the existing PIB are shown through strikethrough (remove) and red (add) text.)

Enhanced Driver's Licence (EDL) / Enhanced Identification Card (EIC) Information Program

Description: This bank describes personal information that is collected from a provincial or territorial EDL/EIC program and used in support of the EDL/EIC Program admissibility determination. The EDL/EIC Program is a voluntary program that is available to Canadian citizens. ~~The EDL/EIC Program is one of the Government of Canada's responses to the U.S. Western Hemisphere Travel Initiative. The Program is the responsibility of the participating provinces/territories.~~ EDL / EIC information is collected by ~~p~~Participating provinces/territories and provided ~~determine the applicants' eligibility and collect required information.~~ The provinces/territories disclose specific personal information to the Canada Border Services Agency (CBSA). The CBSA will store that information in its EDL/EIC database to enable Border Services Officers to verify the validity of the document and the identity of the traveller, when it is presented for cross border travel. In addition, the information will be available for query by ~~assist United States~~ (U.S.) Customs and Border Protection (CBP) in determining the admissibility of an EDL holder for entry into the U.S. ~~As such, when a holder presents an EDL/EIC at a U.S. border, CBP will request the information from the EDL/EIC database held by the Canada Border Services Agency (CBSA).~~ U.S. CBP will use this information to verify the validity of the card, as well as the citizenship and identity of the holder. The personal information collected from ~~by participating provinces and territories~~ may include: Full Name (first name, last name), Birth date, Gender, Citizenship, Digital image (holder's photo), Tag Identification number (TID), Optical Character Recognition unique identifier (Encoded Document Number (EDN)-used in Machine Readable Zone (MRZ)), Radio Frequency Identification ((RFID), Tag value), Serial Number (if applicable), Document type (EDL or EIC), Issuing Country, Issuing Jurisdiction (province), Expiration Date and Issuance Date.

Class of Individuals: Canadian citizens that are or were Enhanced Driver Licence/Enhanced Identification Card holders.

Purpose: The personal information related to the EDL/EIC program will be used to facilitate cross border travel at U.S. and Canadian land ports of entry. To facilitate this primary purpose, the information will be made available for query purposes to U.S. CBP and the CBSA. ~~is used to administer the EDL/EIC information exchange between the Canada Border Services Agency (CBSA) and CBP.~~ Personal Information is collected pursuant to *section 5(1) of the Canada Border Services Agency Act* as well as sections 4(2), 18(1) and 19(1) of the *Immigration and Refugee Protection Act* and section 11 of the *Customs Act*.

Consistent Uses: The information may be used or disclosed for the following purposes: administration, enforcement and evaluation of the EDL/EIC Program for border crossing purposes. Information may be shared with: Federal Institution(s): Immigration, Refugees and Citizenship Canada (IRCC) ~~Citizenship and Immigration Canada (CIC).~~ The Canada Border Services Agency (CBSA) enters information related to lost/stolen/fraudulent (LSF) EDLs/EICs into the LSF module of (CBSA'S Interdiction and Border Alerting System (IBAS)), in order to report lost/stolen/fraudulent Enhanced Driver's Licences/Enhanced Identification Cards. ~~Government(s) of (a) foreign state(s) or of (an) institutions thereof.~~ Full Name (first name, last name), Birth date, Gender, Citizenship, Digital image (holder's photo), Tag Identification number (TID), Optical Character Recognition unique identifier (Encoded Document Number (EDN) - used in Machine Readable Zone (MRZ)), Radio Frequency Identification ((RFID) Tag value), Serial Number (if applicable), Document type (EDL or EIC), Issuance Date, Expiration Date, Licence Status and Status Changes (Card Status Reason Code), Licence Issuing Jurisdiction, Issuing Country may be shared with the U.S. Government (U.S. Customs Border Protection) when seeking entry into the United States. For the details on U.S. CBP's handling of the information collected upon entry into the U.S., refer to the Border Crossing Information System of Records Notice (BCI SORN) 73, Reg. 43,457. Province(s) or (an) institution(s) thereof: Personal information may be shared between the Canada Border Services Agency (CBSA) and the individual participating provinces/territories, which currently consist of British Columbia, Manitoba and Ontario ~~and Quebec.~~ The Optical Character Recognition unique identifier (also referred to as Encoded Document Number (EDN), EDL issuance date, Document type (EDL or EIC), Licence Issuing Jurisdiction (PT), Issuing Country as well as the reason code (Lost/stolen issued, lost/stolen blank card, cancelled/revoked, fraudulently issued/obtained, etc.) may be shared ~~with~~by provinces/territories where changes occur to the status of the EDL. In these instances, the provinces/territories are responsible to gather and send to the Canada Border Services Agency (CBSA) information on ~~lost, stolen, or fraudulent (LSF) EDLs, EDLS where the holder has deceased, and EDLs that are no longer valid (i.e. cancelled).~~

Retention and Disposal Standards: EDLs/EICs are retained by the Canada Border Services Agency (CBSA) as long as they are deemed to be active by the province or territory that issued them. When an EDL/EIC is deemed to be inactive (expired, lost, stolen, surrendered, no longer valid, cancelled, fraudulently obtained, holder deceased) by the province or territory that issued it, the province or territory notifies the Canada Border Services Agency (CBSA). The Canada Border Services Agency (CBSA) retains EDL/EIC records for two (2) years following the last administrative action (i.e. when the Canada Border Services Agency (CBSA) is advised that the card is no longer active for border-crossing purposes). The information is then destroyed according to the Government of Canada's secure disposal requirements.

RDA Number: 2000-0333 2015/008

Related Record Number: CBSA IST 004

TBS Registration: 20090946

Bank Number: CBSA PPU 061

Legal Authority for Program or Activity:

Enabling authority for the use, collection and disclosure of information by the CBSA is the *Immigration and Refugee Protection Act*, sections 4(2), 18(1) and 19(1).

4. (2) The Minister of Public Safety and Emergency Preparedness is responsible for the administration of this Act as it relates to

- (a) examinations at ports of entry;
- (b) the enforcement of this Act, including arrest, detention and removal;
- (c) the establishment of policies respecting the enforcement of this Act and inadmissibility on grounds of security, organized criminality or violating human or international rights; or
- (d) declarations referred to in section 42.1.

18 (1) Every person seeking to enter Canada must appear for an examination to determine whether that person has a right to enter Canada or is or may become authorized to enter and remain in Canada.

19 (1) Every Canadian citizen within the meaning of the *Citizenship Act* and every person registered as an Indian under the *Indian Act* has the right to enter and remain in Canada in accordance with this Act, and an officer shall allow the person to enter Canada if satisfied following an examination on their entry that the person is a citizen or registered Indian.

Enabling authority is also found in the *Customs Act*, section 11.

11 (1) Subject to this section, every person arriving in Canada shall, except in such circumstances and subject to such conditions as may be prescribed, enter Canada only at a customs office designated for that purpose that is open for business and without delay present himself or herself to an officer and answer truthfully any questions asked by the officer in the performance of his or her duties under this or any other Act of Parliament.

(2) Subsection (1) does not apply to any person who has presented himself or herself outside Canada at a customs office designated for that purpose and has not subsequently stopped at any other place prior to his or her arrival in Canada unless an officer requires that person to present himself or herself to the officer.

(3) Subject to this section, every person in charge of a conveyance arriving in Canada shall, except in such circumstances and subject to such conditions as may be prescribed, ensure that the passengers and crew are forthwith on arrival in Canada transported to a customs office referred to in subsection (1).

(4) Subsection (3) does not apply to any person in charge of a conveyance transporting passengers and crew all of whom have presented themselves outside Canada at a customs office designated for that purpose and have not subsequently stopped at any other place prior to their arrival in Canada unless an officer requires that person to comply therewith.

(5) Subsections (1) and (3) do not apply to any person who enters Canadian waters, including the inland waters, or the airspace over Canada while proceeding directly from one place outside Canada to another place outside Canada unless an officer requires that person to comply with those subsections.

(6) Subsection (1) does not apply to a person who

- (a) holds an authorization issued by the Minister under subsection 11.1(1) to present himself or herself in a prescribed alternative manner and who presents himself or herself in the manner authorized for that person; or
- (b) is a member of a prescribed class of persons authorized by regulations made under subsection 11.1(3) to present himself or herself in a prescribed alternative manner and who presents himself or herself in the manner authorized for that class.
- (7) Notwithstanding that a person holds an authorization under subsection 11.1(1) or is authorized under the regulations made under subsection 11.1(3), an officer may require a person to present himself or herself in accordance with subsection (1).

Summary of the project, initiative, or change:

In 2008, this initiative had two PIAs completed: January 2008 focussed on the piloted roll-out of the initiative and December 2008 assessed the wider scale roll-out as well as addressing the privacy concerns detailed in a joint resolution issued February 5, 2008 by Canada's Federal-Provincial-Territorial Privacy Commissioners.

Currently, there are three provinces issuing EDLs: Ontario, Manitoba and British Columbia. Canadian EDLs can be used by a Canadian to enter into the U.S. The CBSA hosts the secure database required to verify the EDL/EIC and facilitates the transmission of the traveller information to U.S. CBP officials. Canadian BSOs have no access to the information from the EDL/EIC database at this time.

This PIA will focus on the implementation of RFID readers at select Canadian Ports of Entry (POE). This technology will allow CBSA BSOs to retrieve the EDL/EIC information stored in the secure database when a cardholder seeks entry to Canada. As Quebec closed their EDL program to new applicants in October 2014, the CBSA will not be accessing Quebec EDL data.

SECTION 2 - RISK AREA IDENTIFICATION AND CATEGORIZATION

Type of Program or Activity	Level of Risk
<p>Program or activity that does NOT involve a decision about an identifiable individual</p> <p>Personal information is used strictly for statistical / research or evaluations including mailing list where no decisions are made that directly have an impact on an identifiable individual.</p> <p>The Directive on PIA applies to administrative use of personal information. The Policy on Privacy Protection requires that government institutions establish an institutional Privacy Protocol for addressing non-administrative uses of personal information. <i>The CBSA Privacy Protocol must be implemented. Contact the ATI and Privacy Division before continuing the PIA.</i></p>	<input type="checkbox"/> 1
<p>Administration of Programs / Activity and Services</p> <p>Personal information is used to make decisions that directly affect the individual (i.e. determining eligibility for programs including authentication for accessing programs/services, administering program payments, overpayments, or support to clients, issuing or denial of permits/licenses, processing appeals, etc...).</p>	<input checked="" type="checkbox"/> 2
<p>Compliance / Regulatory investigations and enforcement</p> <p>Personal information is used for purposes of detecting fraud or investigating possible abuses within programs where the consequences are administrative in nature (i.e. a fine, discontinuation of benefits, audit of personal income tax file or deportation in cases where national security and/or criminal enforcement is not an issue).</p>	<input checked="" type="checkbox"/> 3
<p>Criminal investigation and enforcement / National Security</p> <p>Personal information is used for investigations and enforcement in a criminal context (i.e. decisions may lead to criminal charges/sanctions or deportation for reasons of national security or criminal enforcement).</p>	<input checked="" type="checkbox"/> 4
<p>Details: Information collected by the provinces strictly for the issuance of EDLs and provided to the CBSA would be used to facilitate cross border land and water travel back and forth between Canada and the U.S. and would not be used for any other purpose. However, at the point of border crossing, the information would form a part of the Traveller Processing records. Those records do have the potential to be used to enforce residency requirements under the <i>Immigration and Refugee Protection Act</i>, import / export limits under the <i>Customs Act</i>, criminal investigations / security (where applicable) and potentially, provided to Other Government Departments (OGDs) under information sharing agreements, for the enforcement of programs with residency requirements.</p>	

Type of Personal Information Involved and Context	Level of Risk
Only personal information, with no contextual sensitivities, collected directly from the individual or provided with the consent of the individual for disclosure under an authorized program. For example: General licensing, or renewal of travel documents or identity documents.	<input type="checkbox"/> 1
Personal information, with no contextual sensitivities after the time of collection, provided by the individual with consent to also use personal information held by another source. For example: An application process with a requirement for independent verification of certain non-sensitive factual details.	<input type="checkbox"/> 2
Social Insurance Number, medical, financial or other sensitive personal information and/or the context surrounding the personal information is sensitive. Personal information of minors or incompetent individuals or involving a representative acting on behalf of the individual. For example: An individual's name on a particular list may reveal sensitive information on the health, financial situation, religious or lifestyle choices of that individual.	<input checked="" type="checkbox"/> 3
Sensitive personal information, including detailed profiles, allegations or suspicions, bodily samples and/or the context surrounding the personal information is particularly sensitive. For example: Personal information that reveals intimate details on the health, financial situation, religious or lifestyle choices of the individual and which, by association, reveals similar details about other individuals such as relatives.	<input type="checkbox"/> 4
Details: Collection of the information from the individual is completed by one of the three provinces, in order to issue an EDL/EIC. Once issued, the province provides the CBSA with: full name (first, last), birth date, gender, digital image (holder's photo), citizenship (must be Canadian), licence issuing jurisdiction (province), issuing country (Canada), EDL issuance date, EDL expiry date, licence/card status (i.e., issued, lost, stolen, etc.), serial number, TID, Optical Character recognition unique identifier EDN/Rfid unique identifier.	

In addition to the availability of verification information in the CBSA database, the EDLs/EICs themselves have personal information available directly on the document. This information is used to verify the validity of the document.

Use of Enhanced Driver's Licence and Enhanced Identification Card Information by the Canada Border Services Agency

PIA

Front of EDL	Back of EDL
<ul style="list-style-type: none"> Name Address Birth Date Driver Licence Number Driver Licence Class Issue and Expiry Dates Picture of Entitled Holder Height, Weight, Eye Colour, Hair Colour, Gender RFID chip (embedded) Citizenship (denoted by the "C") Signature of EDL holder 	<ul style="list-style-type: none"> Restriction and Endorsement Codes Tag Identification Number (TID), Optical Character Recognition unique identifier EDN RFID unique identifier (ID)

Program or Activity Partners and Private Sector Involvement

Level of Risk

Within the CBSA (amongst one or more programs within the CBSA)

☒ 1

With other federal institutions

☒ 2

With other or a combination of federal/ provincial and/or municipal government(s)

☒ 3

Private sector organizations or international organizations or foreign governments

☒ 4

Details: Information is collected by the three participating provinces and sent to the CBSA in order to facilitate use of the records by U.S. CBP, during the border crossing process. With the installation of RFID technology, it is the intention of the CBSA to make the database information available to CBSA BSOs to enable the use of EDLs by Canadian citizens as proof of identification/evidence of citizenship.

Duration of the Program or Activity

Level of risk

One time program or activity

☐ 1

Typically involves offering a one-time support measure in the form of a grant payment as a social support mechanism.

Short-term program

☐ 2

A program or activity that supports a short-term goal with an established "sunset" date.

Long-term program

☒ 3

Existing program that has been modified or is established with no clear "sunset".

Details: CBSA has been collecting the EDL/EIC information and making it available to U.S. CBP since 2008. It is the intention that this will be a long-term activity.

Program Population

Level of Risk

- The program affects certain employees for internal administrative purposes. ☐ 1
- The program affects all employees for internal administrative purposes. ☐ 2
- The program affects certain individuals for external administrative purposes. ☒ 3
- The program affects all individuals for external administrative purposes. ☐ 4

Details: This initiative will affect individuals who hold EDLs/EICs and present themselves at an RFID-enabled POE. As of July 2016, there were more than 500,000 Canadian EDL/EICs in active circulation. This number has remained steady since their introduction in 2008/2009.

Technology and Privacy

- 6.1 Does the new or modified program or activity involve the implementation of a new electronic system, software or application program including collaborative software (or groupware) that is implemented to support the program or activity in terms of the creation, collection or handling of personal information? ☒ YES ☐ NO

- 6.2 Does the new or modified program or activity require any modifications to IT legacy systems and / or services? ☒ YES ☐ NO

- 6.3 Does the new or modified program or activity involve the implementation of one or more of the following technologies:

6.3.1 Enhanced identification methods:

- ☒ YES ☐ NO

Details: Currently, U.S. CBP uses RFID technology to read EDLs and render the information on their screens in order to make land border crossing as efficient as possible. It is the intention of the CBSA to enable technology at select Canadian border crossings, similar to the U.S. in that they employ RFID technology at their POEs.

6.3.2 Use of Surveillance:

- ☐ YES ☒ NO

Details: Enabling RFID technology in the travel document is a requirement of the U.S. Western Hemisphere Travel Initiative (WHTI) and is not negotiable.

While RFID technology is used to transmit the information to the CBSA BSO, it is limited to when the person presents themselves at the land POE. It would not be used by the CBSA as a method of surveillance. It is noteworthy that the EDLs/EICs are issued by the provinces (not the CBSA) enabled with RFID technology and already used by U.S. CBP. The current changes to the program are to enable use of the card as identification for those returning to Canada via land POEs.

The RFID antenna will be activated when a sensor is triggered by the approach of a vehicle in an RFID-enabled primary inspection lane. Once activated, the antenna will read the chip in the EDL/EIC, retrieve a unique tag identifier (ID), and transmit it to the CBSA systems. Chips in RFID-enabled travel documents that are not acceptable for border crossing will be automatically filtered out by CBSA systems.

There is no personal information contained within the RFID chip, only a Tag Identification (TID) number embedded by the manufacturer to prevent cloning by ensuring that the TID that is returned when a card is read matches the embedded TID; and an RFID unique identifier containing 96 bits of 0s and 1s to retrieve information from the EDL database.

When the unique tag ID is received by CBSA systems, a process will be activated to send a request to the relevant secure database, validated and the corresponding traveller tombstone information will be retrieved. The information that is retrieved from the database will present the biographic and biometric (photo) information and query results to the BSO.

In order to reduce the risk of surreptitious location tracking of individuals carrying an EDL, the provincial issuing authorities have been advised to issue their EDLs/EICs with a protective sleeve. This sleeve prevents the skimming of data from the RFID tag. Furthermore, RFIDs are only readable at a short distance and can only be read by RFID readers when taken out of the protective sleeve (the tags are passive and do not transmit information).

Initially, 13 Canadian land POEs will be enabled with RFID readers. With successful deployment, additional POEs may be added. The 13 initial POEs are:

Additional sites will be added in future that will function in the same manner as the 13 sites above.

6.3.3 Use of automated personal information analysis, personal information matching and knowledge discovery techniques:

☒ YES
☐ NO

Details: Information held in the CBSA database is held, with no administrative decision or data matching until an individual uses the EDL/EIC to cross the border at a land POE. At that point, the U.S. CBP Officer or the CBSA BSO would review the information presented and compare it with the information contained in the database. The data matching activity is limited to matching the information presented by the traveller on the card to the information captured in the existing database. The resulting administrative decision would be whether the BSO allows the person to enter the country, or not.

Personal Information Transmission

Level of Risk

The personal information is used within a closed system.

☐ 1

No connections to Internet, Intranet or any other system. Circulation of hardcopy documents is controlled.

Use of Enhanced Driver's Licence and Enhanced Identification Card Information by the Canada Border Services Agency

PIA

The personal information is used in system that has connections to at least one other system. ☒ 2

The personal information is transferred to a portable device or is printed. ☐ 3

USB key, CD-Rom, laptop computer, any transfer of the personal information to a different medium.

The personal information is transmitted using wireless technologies. ☐ 4

Details: The EDL-issuing provinces use either MQSeries or IBM WebService to send the EDL data to the CBSA encrypted using Public Key Infrastructure -PKI). MQSeries is an International Business Machines Corporation (IBM) software family whose components are used to tie together other software applications so that they can work together. This type of application is often known as business integration software or middleware. It allows independent and potentially non-concurrent applications on a distributed system to securely communicate with each other.

Use of Enhanced Driver's Licence and Enhanced Identification Card Information by the Canada Border Services Agency

PIA

Risk Impact to the CBSA

Level of Risk

Managerial harm.

☐ 1

Processes must be reviewed, tools must be changed, change in provider / partner.

Organizational harm.

☐ 2

Changes to the organizational structure, changes to the organizations decision-making structure, changes to the distribution of responsibilities and accountabilities, changes to the program activity architecture, departure of employees, reallocation of HR resources.

Financial harm.

☐ 3

Lawsuit, additional moneys required reallocation of financial resources.

Reputation harm, embarrassment, loss of credibility.

☒ 4

Decreased confidence by the public, elected officials under the spotlight, institution strategic outcome compromised, government priority compromised, impact on the Government of Canada Outcome areas.

Details: The personal information collected by the CBSA is held in the database to facilitate cross border travel. A breach of the information could cause concern among EDL/EIC holders (and the general public) regarding the ability of the CBSA to safeguard personal information in general. The EDL/EIC data is held in a secure database, and can only be accessed by authorized users.

Risk Impact to the Individual or Employee

Level of Risk

Inconvenience.

☒ 1

Reputation harm, embarrassment.

☐ 2

Financial harm.

☒ 3

Physical harm.

☐ 4

Details: While identity theft appears to be possible with even a minimal amount of personal information, the value of the information transmitted for the EDL/EIC process is limited.

SECTION 3 - ANALYSIS OF PERSONAL INFORMATION ELEMENTS

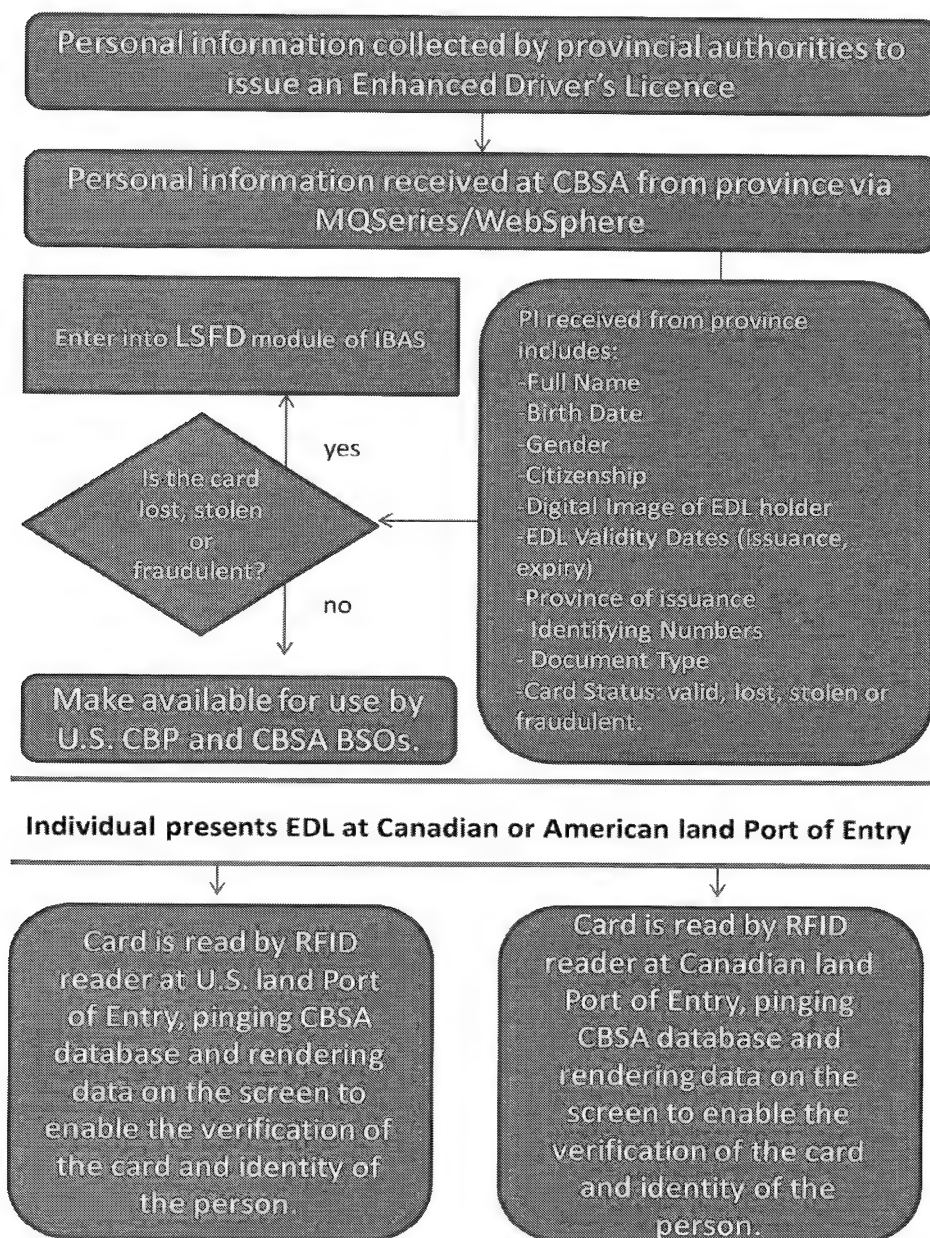
Personal Information Elements and Sub-elements

Category Of Personal Information	Personal Information Element	Personal Information Sub-Element	Format	Purpose / Necessity of Element
Name	1) Name	1) First name / middle initial / last name	Electronic, from the province and available on the EDL/EIC	To identify clients in the database at the time of border crossing.
Contact information	2) Home address	2) Street name / street number / city / province / postal code	Available only on the EDL/EIC	To verify the validity of the card and the identity of the person crossing the border. This information is viewed by the BSO when the card is presented at a Port of Entry.
Birth date	1) Day, Month and Year of birth		Electronic, from the province and available on the EDL/EIC	To verify the validity of the card and the identity of the person crossing the border.
Biographical Information	1) Detailed Physical Characteristics	1) Height 2) Weight 3) Eye Colour 4) Gender	Gender is provided electronically and held in the database. Other biographical elements are available only on the EDL/EIC.	To verify the identity of the person crossing the border. Other than gender, biographical information is viewed by the BSO when the card is presented at a POE. Only gender is recorded in the CBSA databases, unless there was a required referral for intelligence and enforcement.
Identifying Numbers	Individually assigned reference numbers, relatable to an individual through verification in the database.	1) Enhanced Driver's Licence or Enhanced Identification Card Number 2) Optical Character Recognition unique identifier (EDN)	Electronic, from the province; EDL/EIC Number available on the EDL/EIC.	Scan EDL/EIC and retrieve information quickly and accurately for use by the BSO when the EDL/EIC is presented as identification for border crossing.

		3) RFID unique identifier (ID)		
EDL Validity Dates	1) Date of Issuance 2) Date of Expiry		Electronic, from the province and available on the EDL/EIC.	To verify the validity of the card.
Visual Image of EDL holder	1) Photo of the face		Electronic, from the province and available on the EDL/EIC	To verify the identity of the person crossing the border.
Citizenship of Individual	1) Holders of the card must be Canadian citizens, therefore it is inferred that having the card denotes citizenship	1) Denoted through the capital "C" on the card.	Electronic, from the province and available on the EDL/EIC	To meet the U.S. criteria for an enhanced border crossing document and verify identity for re-entry to Canada.
Licence Status	In addition to active status, EDL can be designated as lost, stolen, fraudulently issued, fraudulently obtained, deceased card holder and/or revoked status.	1) Card status 2) Card status reason code	Electronic, from the province	To ensure only active cards are accepted in cross border travel.

SECTION 4 - FLOW OF PERSONAL INFORMATION

4.1 Data Flow Model - Diagrams



Once the card is read at the border, the information becomes part of a record of passage and information related to the border crossing would be considered traveller processing information. This information can be stored in one or more CBSA databases:

- Integrated Customs Enforcement System (ICES)
- Integrated Primary Inspection Line (IPIL)
- Passenger Information System (PAXIS)
- Telephone Reporting Centre System (TRCS)
- Secondary Processing System (SP)
- Passage History Database (PH)
- Occurrence Reporting System (ORS)
- Intelligence Management System (IMS)
- Integrated Border Query (IBQ)
- Canadian Police Information Centre (CPIC)
- National Crime Information Center (NCIC)
- Client Status Query (CSQ)
- Modern War Crimes System (MWCS)
- Secure Tracking System (STS)
- Support System for Intelligence (SSI)
- National Case Management System (NCMS)
- Global Case Management System (GCMS)
- Automated Fingerprint Identification System (AFIS)

Once the information is entered into CBSA data bases to form a record of entry, different retention schedules and disclosures may occur.

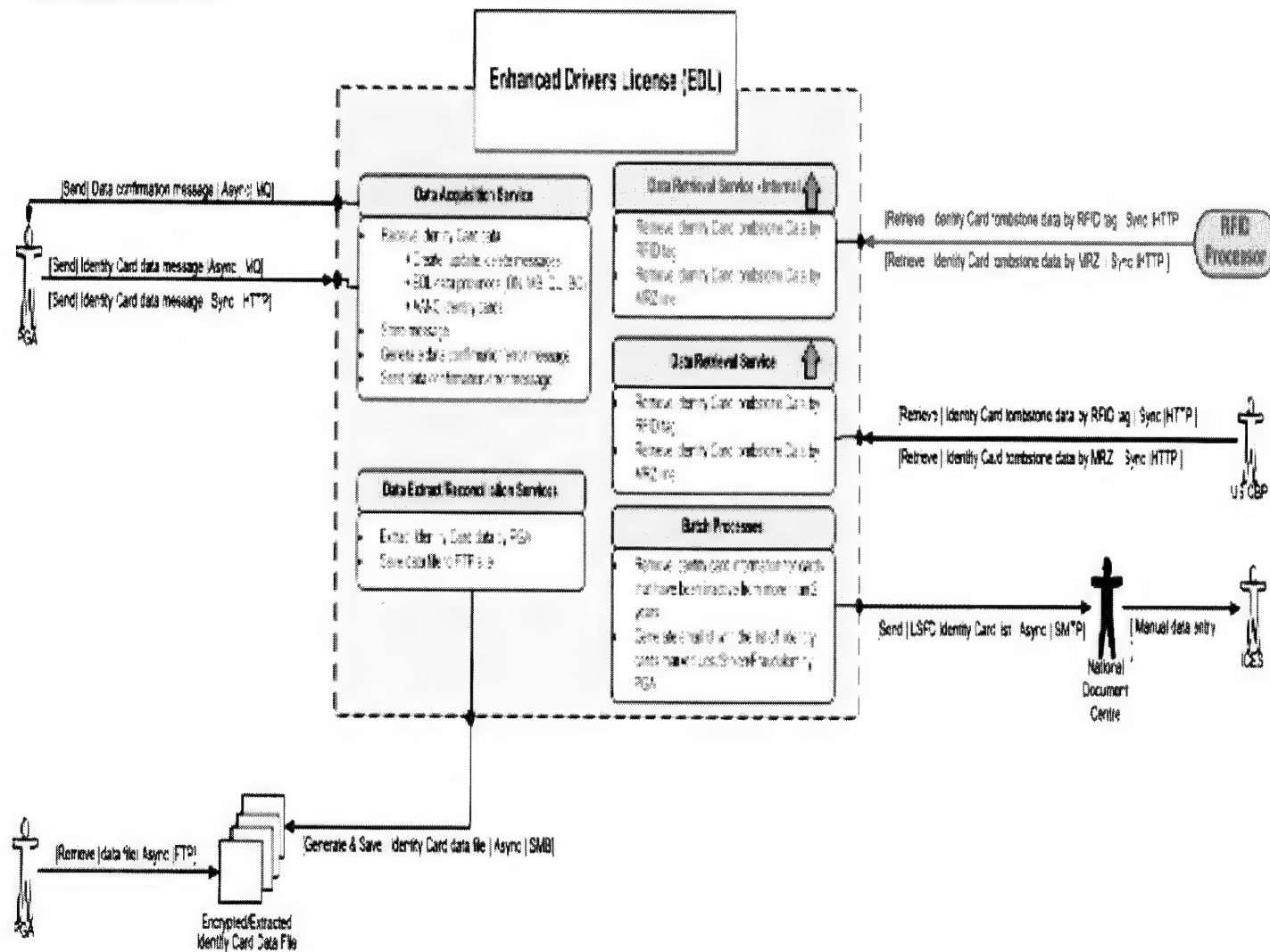
Use of Enhanced Driver's Licence and Enhanced Identification Card Information by the Canada
Border Services Agency

PIA

Data Exchange

Presentation of EDL at Canadian POE

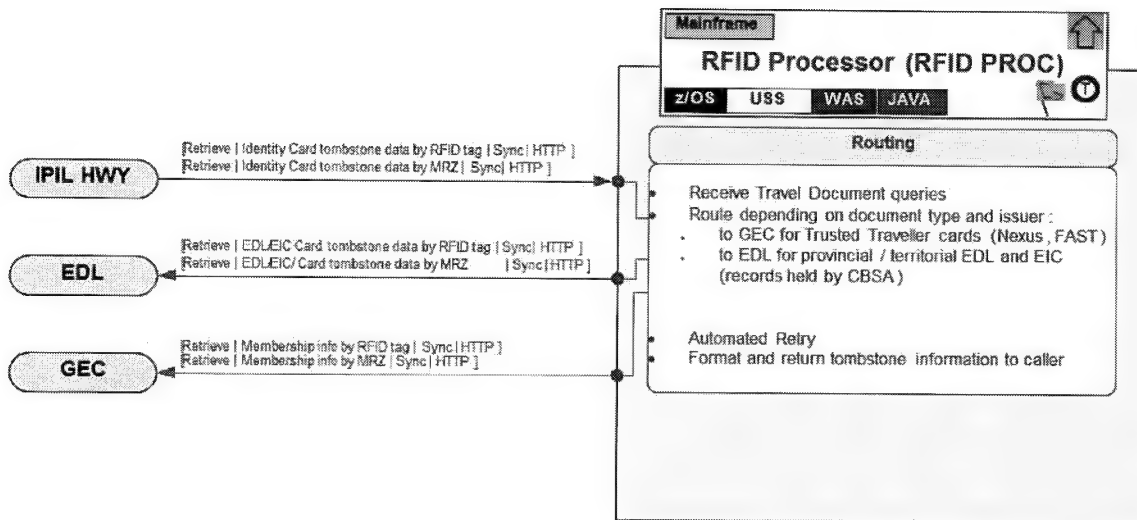
EDL - Future State - After RFID Initiative



Use of Enhanced Driver's Licence and Enhanced Identification Card Information by the Canada
Border Services Agency

PIA

Interaction with RFID Processor



4.2 Data Flow Model - Table

SOURCE	IDENTIFY THE SOURCE
Provincial governments of Ontario, Manitoba and British Columbia	Information is sent from the provinces to the CBSA and held in a database to enable verification of the validity of the document and facilitate land/water border crossing. For example, Manitoba's Applicant Guide informs applicants that "Your personal information will be transmitted by Manitoba Public Insurance to the CBSA by a secure, encrypted network."
The individual	At the point of border crossing via land/water POE, the EDL holder presents the document to demonstrate their identity. If seeking entry into the U.S. the EDL also identifies their Canadian citizenship.

4.3 Internal Use and Disclosure

Once information becomes traveller processing information (when an individual presents their card to re-enter Canada), the information is available for multiple uses.

Program	Personal information bank
Traveller Processing	Traveller Processing CBSA PPU 1101: The personal information collected may include: name, contact information, citizenship, date of birth, place of birth, gender, date and time of entry, POE, travel document type (e.g., passport) including identification number and country of issuance, membership program information – i.e. NEXUS, residency, and GCMS ID(Unique Client Identifier (UCI)) number. In the land mode, passenger vehicle license plate information is collected. Personal Information can be stored in the following databases:

	<ul style="list-style-type: none"> • Integrated Customs Enforcement System (ICES) • Integrated Primary Inspection Line (IPIL) • Passenger Information System (PAXIS) • Telephone Reporting Centre System (TRCS) • Secondary Processing System (SP) • Passage History Database (PH) • Occurrence Reporting System (ORS) • Intelligence Management System (IMS) • Integrated Border Query (IBQ) • Global Case Management System (GCMS) • Canadian Police Information Centre (CPIC) • National Crime Information Center (NCIC) • Client Status Query (CSQ) • Modern War Crimes System (MWCS) • Secure Tracking System (STS) • Support System for Intelligence (SSI) • National Case Management System (NCMS), and • Automated Fingerprint Identification System (AFIS).
Intelligence Program	<p>Intelligence Program CBSA PPU 035: Personal information may include name, contact information, biographical information, biometric information, citizenship status, credit information, criminal checks/history, date of birth, educational information, financial information, travel/identity documents, personal identification numbers, physical attributes, place of birth, signature, import/export information, customs infractions and/or seizures, traveller history and immigration violations.</p> <ul style="list-style-type: none"> • Personal Information may be stored in the following systems: • Intelligence Management System (IMS) • the Support System for Intelligence (SSI) • Secure Tracking System (STS) • Integrated Customs Enforcement System (ICES) • National Case Management System (NCMS) • Global Case Management System (GCMS) • Canadian Police Information Center (CPIC)

CBSA Uses Permitted by the Provinces

Memoranda of Understanding (MOU)

Amendments made to the MOUs between the provinces (i.e., BC, Manitoba and Ontario) and the CBSA now authorize the CBSA to access the information held in the CBSA's EDL database on their behalf. The limitations on use are expressed in different sections for each of the provinces and the wording may be slightly different. The province of Quebec chose not to participate and as such, the CBSA will not access information related to holders of the Quebec EDL. The number of active Quebec EDLs will diminish over time as they expire and cannot be renewed.

General

Once the information forms a record of passage, details regarding the border crossing, including identifying references to the EDL itself (ID number, type of document, province of issuance, etc.) are entered into relevant CBSA databases and the information can be used for multiple intelligence and enforcement purposes. This would be the same process regardless of whether a traveller uses an EDL or a passport to enter the U.S. or Canada.

4.4 External Use and Disclosure

EDL information is disclosed under limited circumstances; however, once an individual uses their EDL to facilitate cross border travel, the information becomes a record of the border crossing.

4.5 Retention / Storage

Canada Border Services Agency	<p>The CBSA particular Personal Information Bank EDL/EIC information cites an RDA of 2015-008. The corresponding retention period published in the PIB states, "EDLs/EICs are retained by CBSA as long they are deemed to be active by the province or territory that issued them. When an EDL/EIC is deemed to be inactive (expired, lost, stolen, surrendered, no longer valid, cancelled, fraudulently obtained, holder deceased) by the province or territory that issued it, the province or territory notifies the CBSA. The CBSA retains EDL/EIC records for two (2) years following the last administrative action (i.e. when the CBSA is advised that the card is no longer active for border-crossing purposes). The information is then destroyed according to the Government of Canada's secure disposal requirements."</p> <p>The MOU divides retention into three categories: active, inactive and Lost/Stolen/Fraudulent. However, the MOU also states that EDLs become inactive when they are reported lost or stolen. The retention standards for the two categories are different.</p> <p>Active EDL information will be stored in the CBSA database for as long as the EDL remains active;</p> <p>Inactive EDLs are considered inactive when they are reported lost or stolen, when they are surrendered, no longer valid, cancelled or when the cardholder is deceased. EDL information for inactive EDLs will be stored in the CBSA database for two years following the last administrative action on the EDL information, and then removed from that system completely according to the Government of Canada's secure disposal requirements.</p> <p>Lost/Stolen/Fraudulent EDL information that is stored in CBSA databases is retained for a period of 10 years based on the CBSA Disposition Authority 2015/008 under the CBSA Program Alignment Architecture (PAA) Section 1.1 (Intelligence).</p>
Non-federal institutions and private sector	
Province of Ontario	There is no reference to retention in the EDL Applicant Guide.

	The MOU states that the province will "store information in the licencing and control system, on microfilm/fiche, and in the appropriate audit and reconciliation or secure storage database in order to monitor EDL applications and card issuance, respond to requests for information by authorized parties, and to CBSA and IRCC with information required by US CBP and quality assurance processes. The province will retain EDL information indefinitely to support the EDL program and any enquiries and investigations."
Province of Manitoba	No timelines provided. EDL Applicant Guide states: Information that is collected about you as part of this program will be kept by Manitoba Public Insurance to maintain your EDL or EIC record for as long as your card is valid and, even if your application was denied or your card expires or is cancelled, to prevent identity theft and fraudulent applications for Manitoba EDLs and EICs. This information will be kept in accordance with the requirements of Manitoba's <i>Freedom of Information and Protection of Privacy Act</i> .
Province of British Columbia	There is no reference to retention in the EDL Applicant Guide.

The Province of Manitoba provides notice to EDL/EIC applicants regarding the retention of their personal information once it is disclosed to the CBSA and subsequently to U.S. CBP. The EDL Applicant Guide states,

"For CBSA, information for "active" EDLs and EICs (i.e., ones that can be used to cross the United States border) will be stored in CBSA's EDL and EIC database for as long as the card remains active. If your card becomes "inactive" (for example, it is lost, stolen, cancelled, etc.), the CBSA will keep your information in its database for two years. If there has been no activity on the card over the two-year period, the information will then be removed from the EDL and EIC database according to the Government of Canada's secure disposal requirements."

"If you have used your EDL or EIC to enter the United States, United States CBP will have stored information that was sent to it by CBSA when you crossed in its Border Crossing Information (BCI) system. The BCI system is subject to the retention requirements of the US government, which require that information on Canadian citizens (and other foreign nationals) be maintained by CBP for 75 years for border-screening and law enforcement purposes. Regardless of whether you used an EDL, an EIC or a passport to cross the border, information from the document(s) that you presented will be stored in the BCI and subject to the same 75 year retention requirement."

EDL / EIC information is collected and used by the provinces to licence and manage the drivers who are resident in their provinces. The primary purpose of the licencing drivers is not to facilitate border crossing and, as such, the retention of the information by the provinces cannot be dictated by the border crossing use. In addition, as the primary collector of the information, the provinces would be responsible for notifying applicants regarding their intended retention period.

The MOUs makes destruction obligations clear, but do not specify the method of destruction. By way of example, the MOU with Manitoba states: "Each Participant to this Annex agrees that EDL information collected electronically must be destroyed in a way to make it irretrievable, not simply erased from databases, in accordance with their respective policies and laws."

4.6 Other Possible Considerations

Identify the areas, groups and individuals who access and handle the personal information:

Within CBSA, no individual has easy access to the EDL client data. However, the Traveller Processing Enhancements Unit can ask for client data to be pulled from the database with director level approval. This would be done solely for troubleshooting if provinces have problems.

This chart reflects the access and handling provisions for the information, after negotiation with the provinces. It is not the intention of the CBSA to allow any access to the information by CBSA officials until the provinces are in agreement with the use of the information.

The CBSA responsible for program or activity:		
Identify Groups or Areas / or Divisions	Positions who have access or use the personal information (where appropriate)	Geographical Location
CBSA Border Services Officers	More than 1000	Land Ports of Entry
Alternative Traveller Processing Systems Unit	Three	National Capital Region
ATIP Officers (in response to a request)	Less than 100	National Capital Region
CBSA ISTB groups: <ul style="list-style-type: none"> Traveller Systems Division – TSD (1&2) Data Management (DM) Consolidated Management Reporting System (CMRS) (Operations support)	Less than 100	National Capital Region
EDL Participating Canadian Provinces: <ul style="list-style-type: none"> British Columbia Manitoba Ontario Québec (Original data provided to CBSA & CBSA to provide in some cases monthly reconciliation data back to each specific partner)	Less than 100	<ul style="list-style-type: none"> British Columbia: Insurance Corporation of British Columbia (ICBC) Manitoba: Manitoba Public Insurance (MPI) Ontario: Ministry of Transportation Ontario (MTO) Québec : Société de l'assurance automobile du Québec (SAAQ)

Use of Enhanced Driver's Licence and Enhanced Identification Card Information by the Canada
 Border Services Agency

PIA

The Document Integrity Unit (DIU) at CBSA NHQ (the "Nat. Intelligence Documents group"). EDL information is sent to them by appropriate partners through their generic email account.	Less than 100	National Capital Region

SECTION 5 - PRIVACY COMPLIANCE ANALYSIS

1. Legal Authority for Collection of Personal Information

Has a legal authority been identified for the collection of personal information for this program or activity?

OPC recommends that section 5(1) of the Canada Border Services Agency Act be interpreted narrowly by CBSA and that agreements that involve the sharing of information of Canadians with foreign states be subject to the utmost scrutiny and be supported by a detailed business case. (part of the Dec 2008 PIA, page 28)

Yes

- 1.1 ☒ Specify the legal authority and briefly explain its connection to the program or activity or how it permits the collection of the personal information:

Two PIAs completed in 2008 as well as the PIB registered for the program document, the *CBSA Act* as the legislative authority for the collection and use of personal information by the EDL initiative. As this PIA is focused on the new use of the information by CBSA BSOs to allow Canadians to use the EDL as proof of their identity, it should be noted that legislative authority is derived from the *IRPA*, sections 4(2), 18(1) and 19(1.) as well as the *Customs Act*, section 11.

IRPA

4. (2) The Minister of Public Safety and Emergency Preparedness is responsible for the administration of this Act as it relates to

- (a) examinations at ports of entry;
- (b) the enforcement of this Act, including arrest, detention and removal;
- (c) the establishment of policies respecting the enforcement of this Act and inadmissibility on grounds of security, organized criminality or violating human or international rights; or
- (d) declarations referred to in section 42.1.

18 (1) Every person seeking to enter Canada must appear for an examination to determine whether that person has a right to enter Canada or is or may become authorized to enter and remain in Canada.

19 (1) Every Canadian citizen within the meaning of the Citizenship Act and every person registered as an Indian under the Indian Act has the right to enter and remain in Canada in accordance with this Act, and an officer shall allow the person to enter Canada if satisfied following an examination on their entry that the person is a citizen or registered Indian.

Customs Act

11 (1) Subject to this section, every person arriving in Canada shall, except in such

circumstances and subject to such conditions as may be prescribed, enter Canada only at a customs office designated for that purpose that is open for business and without delay present himself or herself to an officer and answer truthfully any questions asked by the officer in the performance of his or her duties under this or any other Act of Parliament.

(2) Subsection (1) does not apply to any person who has presented himself or herself outside Canada at a customs office designated for that purpose and has not subsequently stopped at any other place prior to his or her arrival in Canada unless an officer requires that person to present himself or herself to the officer.

(3) Subject to this section, every person in charge of a conveyance arriving in Canada shall, except in such circumstances and subject to such conditions as may be prescribed, ensure that the passengers and crew are forthwith on arrival in Canada transported to a customs office referred to in subsection (1).

(4) Subsection (3) does not apply to any person in charge of a conveyance transporting passengers and crew all of whom have presented themselves outside Canada at a customs office designated for that purpose and have not subsequently stopped at any other place prior to their arrival in Canada unless an officer requires that person to comply therewith.

(5) Subsections (1) and (3) do not apply to any person who enters Canadian waters, including the inland waters, or the airspace over Canada while proceeding directly from one place outside Canada to another place outside Canada unless an officer requires that person to comply with those subsections.

(6) Subsection (1) does not apply to a person who

(a) holds an authorization issued by the Minister under subsection 11.1(1) to present himself or herself in a prescribed alternative manner and who presents himself or herself in the manner authorized for that person; or

(b) is a member of a prescribed class of persons authorized by regulations made under subsection 11.1(3) to present himself or herself in a prescribed alternative manner and who presents himself or herself in the manner authorized for that class.

(7) Notwithstanding that a person holds an authorization under subsection 11.1(1) or is authorized under the regulations made under subsection 11.1(3), an officer may require a person to present himself or herself in accordance with subsection (1).

Yes

1.3 ☒ Is the personal information collected directly related to an operating program or activity?

The personal information is collected as part of Traveller Processing for the facilitation of cross border travel.

2. Necessity to Collect Personal Information

Is each element and sub-element of personal information collected or to be collected necessary to

administer the program or activity?

YES

The EDL Program will fulfill a need for Canadian citizens who prefer to use a commonly-held and less costly document in lieu of a passport for the purposes of entry into the US at a land or water border crossing. All of the information collected from the provinces and collected on the card at the time of border crossing is required for compliance to the WHTI. In fact, almost all of the information is identical to what would be collected if a passport was used to re-enter into Canada.

However, there are unique identifying numbers on the RFID tag that are not associated with any publicly available information which are also collected. For example, while the new Canadian passport will use an RFID technology, it is not the same as the RFID technology in use for the EDL. Each identifying number is mandatory for the use of the EDL in compliance with the WHTI and none of the identifying numbers (even if intercepted) would reveal the identity of the card holder unless an individual also had access to the EDL database.

None of the personal information elements collected would be considered to be more invasive than applying for a Canadian passport and provincial driver's licence.

- 2.1 ☒ Ensure that all personal information necessary to administer the program or activity is listed in the relevant **PIB**.
- 2.2 ☒ AND, implement controls and procedures to ensure the CBSA does not collect more personal information than is necessary for the identified program or activity and that a continuing need exists for that information or its collection.

2.3 Are secondary uses contemplated for the information collected?

No, the information is being collected for immigration purposes and therefore primary to the administration and enforcement of IRPA.

3. Authority for the Collection, Use or Disclosure of the Social Insurance Number

Is the collection of the Social Insurance Number (SIN) necessary to administer the program or activity?

Statutory reference: Section 4 of *Privacy Act*

Policy reference: Section 6.2.13 of *Policy on Privacy Protection* and sections 6.1.1 and 6.2 to 6.4 of *Directive on Social Insurance Number*

YES

- 3.1 ☐ Collection of the SIN must be in compliance with the *Directive on Social Insurance Number* (please check all appropriate boxes below):
- 3.2 ☐ State legal authority for collecting the SIN:

OR, in the absence of a legal authority to collect the SIN:

- 3.3 ☐ Establish explicit authority through legislative amendment(s).
 3.4 ☐ Establish legal authority as outlined in the *Directive on Social Insurance Number*.

AND, if disclosure of the SIN by the CBSA is to occur on a routine or systematic basis

3.4.1 ☐ to another federal institution that is authorized to collect it, or to another level of government, establish an agreement or arrangement that includes specific provisions to limit the use of the SIN.

3.4.2 ☐ to a contractor or other external service provider, establish a contract that includes specific provisions to limit the use of the SIN.

3.5 ☐ AND, ensure that the relevant **PIB** for the program or activity states the authority under which the SIN is collected and the purpose for which it is used.

NO

3.6 ☒ The SIN is not necessary and it will not be collected, used or disclosed to administer the program or activity.

4. Direct Collection - Notification and Consent (as appropriate)

Is personal information collected directly from the individual to whom it relates?

Statutory reference: Sections 4 and 5 of *Privacy Act*

Policy reference: Sections 6.1.1, 6.2.6 and 6.2.9 to 6.2.13 of *Directive on Privacy Practices* and section 6.1.2 and 6.4.1 of *Directive on Social Insurance Number*

YES

- 4.1 ☐ A "**Privacy Notice**" (adapted for either verbal or written communications) must be provided to the individual at the time of collection and it must include the following elements:
- a) The purpose and authority for the collection
 - b) Any uses or disclosures that are consistent with the original purpose.
 - c) Any uses or disclosures that are not related to the original purpose
 - d) Any legal or administrative consequences for refusing to provide the personal information
 - e) That the "individual to whom the information relates" has rights of access to, correction of and protection of personal information under the *Privacy Act*.
 - f) A reference to the **PIB** for the program or activity
 - g) Why the SIN is collected, how it will be used and the consequence of not providing it.

AND, add a "**Consent Statement**" to the "**Privacy Notice**" as appropriate, if the personal information is to be used or disclosed for a purpose other than the original purpose (**Secondary Use**) or a consistent use, or, to authorize indirect collection of personal information.

- 4.2 ☐ The "**Consent Statement**" must include the following elements:
- a) The purpose of the consent and the specific personal information involved.
 - b) In the case of indirect collections, the sources that will be asked to provide the information.
 - c) Uses and disclosures that are not consistent with the original purpose of the collection and for which consent is being sought.

d) Any consequences that may result from withholding consent.

e) Any alternatives to providing consent

- 4.3 ☐ AND, implement controls and procedures to ensure that the CBSA keeps a record documenting whether or not an individual provided consent when it was sought, including a record documenting any withdrawal of consent when applicable.

Additional Consent Considerations (s. 77(1)(m) of the *Privacy Act*):

- ☐ Standards and mechanisms are in place to ensure that the individual has capacity to give consent.

NO

- 4.4 ☒ The personal information necessary for the program or activity is not collected directly from the individual. It is collected indirectly, for example, from another program within the CBSA, or from another institution, government or third party.

The primary method of collection for this initiative is indirect collection of information from the three participating provinces in order to populate the CBSA database and the presentation of EDLs at the border directly by the individual at the point crossing a POE. The EDL cardholder voluntarily presents their EDL to the CBSA to verify the information already held in the CBSA database.

There is limited signage at the border to provide notice to individuals regarding the collection of their personal information. There are no mandatory scripts in place for use by BSOs to provide notice. This issue is not specific to the EDL program.

5. Indirect Collection - Consent or Authority under Sec. 10 of Privacy Regulations

Is personal information collected indirectly from another source with the informed consent of the individual to whom it relates, or from a person authorized to act on behalf of the individual pursuant to section 10 of the Privacy Regulations?

Statutory reference: Sections 4 and 5 of *Privacy Act* and section 10 of *Privacy Regulations*

Policy reference: Sections 6.1.1, 6.2.6 and 6.2.9 to 6.2.13 of *Directive on Privacy Practices* and sections 6.1.2 and 6.4.1 of the *Directive on Social Insurance Number*

YES

- 5.1 ☒ The notice and consent requirements stated at Question 4 apply. Please provide the "**Privacy Notice**" and/or "**Consent Statement**" below:
- 5.2 ☐ AND, implement controls and procedures to ensure the CBSA keeps a record documenting whether or not an individual provided consent when it was sought, including a record documenting any withdrawal of consent when applicable.
- 5.3 ☒ AND, if information is being collected from persons authorized to act on behalf of minors, incompetents or individuals who have been deceased for less than 20 years, implement appropriate mechanisms to ensure that such persons are authorized to act on behalf of individuals who do not have the capacity to provide consent.

While the *Privacy Act* does not require the provision of notice for indirect collections of information, all

three of the provinces participating in this initiative are subject to provincial privacy legislation, and it was agreed upon early in the process that comprehensive privacy notice would be provided to EDL applicants at the point of application. As there is no legislative obligation for the CBSA to provide notice, and the provinces are not subject to the federal Directive on Privacy Practices, any assessment of the notice provided is anecdotal. The provincial applicant guides, containing the Consent Forms each has developed, are included in the Supplementary Documents submitted with this PIA.

NO

5.4 ☐

6. Indirect Collection - Without Notification and Consent

Is personal information collected from another source without notice to or consent from the individual to whom the information relates?

No, while personal information is collected indirectly, there is notice provided at the point of collection and all provinces request direct consent for the disclosure of information to the CBSA.

7. Retention and Disposal of Personal Information

Has Library and Archives Canada approved a records retention and disposal schedule that applies to the personal information?

Statutory reference: Section 12 of *Library and Archives Canada Act*, sections 6, 10 and 11 of *Privacy Act* and section 4 of *Privacy Regulations*

Policy reference: Sections 6.1.3, 6.2.11 to 6.2.13 and 6.2.23 of *Directive on Privacy Practices*

7.1 ☒ Please identify the Record Disposition Authority (RDA) and describe the retention and disposal schedule:

Details: The CBSA particular Personal Information Bank Enhanced Driver's Licence (EDL) / Enhanced Identification Card (EIC) Program fits within the framework of the CBSA Disposition Authority (DA) of 2015/008 issued by Library and Archives Canada in March 2015 (L&A File # 6240-50/C126-2015/008).

The corresponding retention period published in the PIB states, "EDLs/EICs are retained by CBSA as long they are deemed to be active by the province or territory that issued them. When an EDL/EIC is deemed to be inactive (expired, lost, stolen, surrendered, no longer valid, cancelled, fraudulently obtained, holder deceased) by the province or territory that issued it, the province or territory notifies the Canada Border Services Agency (CBSA). The Canada Border Services Agency (CBSA) retains EDL/EIC records for two (2) years following the last administrative action (i.e. CBSA is advised that the card is no longer active for border-crossing purposes). The information is then destroyed according to the Government of Canada's secure disposal requirements."

7.2 ☒ AND, implement controls and procedures to ensure that personal information used to make a decision that directly affects an individual will be retained for a minimum of two years after the last administrative action or, where a request for access to the information has been received, until such time as the individual has had the opportunity to exercise all his/her rights under the Act.

The MOU between the provinces and the CBSA divides retention into three categories: active, inactive and Lost/Stolen/Fraudulent. However, the MOU also states that EDLs become inactive when they are reported lost or stolen. The retention standards for the two categories are different.

Active EDL information will be stored in the CBSA database for as long as the EDL remains active;

Inactive EDLs are considered inactive when they are reported lost or stolen, when they are surrendered, no longer valid, cancelled or when the cardholder is deceased. In accordance with the MOUs with the provinces, an agreement has been established between CBSA and the document issuing authorities that EDL information retention will be limited to two years following the last administrative action on the EDL information. Once the two year time frame has elapsed, the information will be completely removed from the system according to the Government of Canada's secure disposal requirements.

Lost/Stolen/Fraudulent Under standard practices and procedures within the CBSA, EDL information, for a document reported as lost/stolen/fraudulent (LSFD), is stored in CBSA database(s) and is retained for a period of 10 years based on the CBSA Disposition Authority 2015/008 under the CBSA Program Alignment Architecture (PAA) Section 1.1 (Intelligence).

In addition to the CBSA publishing the retention standard, the standard is addressed in the Memoranda of Understanding with each of the issuing provinces. For example, the MOU with the Government of Ontario states that EDLs are deemed inactive when they are expired, fraudulently obtained, reported lost or stolen, surrendered, no longer valid, cancelled or when the EDL holder is deceased. EDL Information for inactive EDLs will be stored in the CBSA database for two years following the last administrative action on the EDL information, and then removed from the system completely according to the Government of Canada's secure disposal requirements.

Manitoba

Information that is collected about you as part of this program will be kept by Manitoba Public Insurance to maintain your EDL/EIC record for as long as your card is valid and, even if your application was denied or your card expires or is cancelled, to prevent identity theft and fraudulent applications for Manitoba EDLs and EICs. The information will be kept in accordance with the requirements of Manitoba's *Freedom of Information and Protection of Privacy Act* and Manitoba's *Archives and Recordkeeping Act*.

British Columbia

The information that's disclosed to CBSA is protected under provisions of the federal *Privacy Act*. Your EDL application information is sent to CBSA after you activate your card or if your card is reported lost, stolen, cancelled or changed. CBSA will store your information in a secure database in Canada and disclose it to the U.S. Customs and Border Protection when you present your EDL card at the U.S. border. The CBSA will use the information for border crossing purposes when you present your EDL/EIC when entering Canada. The CBSA will also retain information about lost, stolen or otherwise invalid EDLs. CBSA will share this information with other agencies only as authorized by law.

Ontario

There are no references to retention in the Ontario Applicant Guide.

7.3 ☐ AND, if the CBSA intends to dispose of personal information that has been used for an administrative purpose prior to the expiration of the two-year minimum retention standard established by the

Privacy Regulations, it must obtain the consent of the individual to whom the information relates before doing so.

- 7.4 ☒ AND, the CBSA must cite the RDA number, the retention period and the disposition standards for the personal information in the relevant PIB.

NO

- 7.5 ☐ Provide a Records Disposition Submission to Library and Archives Canada describing the records containing the personal information for which the institution requires a RDA.
- 7.6 ☐ AND, obtain a RDA from Library and Archives Canada to allow the CBSA, under certain conditions, to dispose of records that no longer have operational utility for the program or activity.
- 7.7 ☐ AND, ensure that all the other applicable requirements listed under "YES" at Question 7 are met.

8. Accuracy of Personal Information

Will measures be adopted to ensure that personal information used by the CBSA for an administrative purpose is as accurate, up-to-date and complete as possible?

Statutory reference: Sections 6, 10 and 11 of *Privacy Act* and sections 10 and 11 of *Privacy Regulations*

Policy reference: Sections 6.1.1 and 6.2.9 to 6.2.16 of *Directive on Privacy Practices*

YES

- 8.1 ☒ Please check any of the following measures that will be adopted to ensure accuracy of the personal information and provide details as requested:
- 8.1.1 ☐ Personal information will be collected directly from the individual to whom it relates or it will be validated with the individual or a person authorized to act on behalf of the individual.
- 8.1.2 ☒ A data-matching process will be used to verify the accuracy of personal information against a "reliable source" (within or outside the CBSA) where this is authorized, or where consent was obtained.

Details: Once an individual uses the EDL / EIC as identification for cross border travel, the details on the card will be verified by the CBSA BSO and/or U.S. CBP. The information on the card is reviewed for accuracy with the cardholder, verifying the information against the information held in the database. If any information appears to be inconsistent, the traveller may be referred for additional processing to clarify or resolve the inconsistency.

- 8.1.3 ☒ In cases where direct collection or consent is not feasible, the CBSA will obtain information from trusted sources (public or private) and verify accuracy against existing personal information before use.

Details: When personal information is received from the provinces, the information will be confirmed via automated methods for format accuracy, omissions and discrepancies. This information is received through indirect collection and will not be used to make an administrative decision that directly affects the individual, until the card holder presents their ID at a land/water POE and the information is verified.

- 8.1.4 ☒ Technological methods will be used to identify errors and discrepancies.

Details: The technology solution incorporates an immediate reconciliation when the data string is received. The reconciliation does not confirm the content of the data string but confirms that CBSA has received the data string that was sent. The province is responsible for ensuring that they receive the appropriate responses back from CBSA.

A reconciliation report will be generated for the provinces for their reconciliation and management of EDL data. In addition, the CBSA, at the request of a province may create a data integrity report, containing that provinces' EDL information and provide it to the province for the purposes of verifying the integrity of the EDL information in CBSA's EDL database. CBSA cannot manipulate EDL data and provinces are responsible for all updates to the EDL records.

8.1.5 ☐ Other

Specify: *(This information is mandatory)*

8.2 ☐ AND, if measures are adopted other than "direct collection or validation with the individual or with a person authorized to act on behalf of the individual", the CBSA must implement appropriate controls and procedures to ensure that:

- a) the technique(s) and the specific source(s) used to validate or update the personal information are documented;
- b) individuals are given the opportunity, whenever possible, to request correction of any inaccurate personal information before the information is used in a decision-making process that affects them;
- c) personal information can only be modified or corrected by those within the CBSA who have the authority to do so;
- d) when personal information is corrected or annotated, the record of personal information indicates the date of the last correction or annotation and the source of the information used to make the correction or annotation; and
- d) when personal information is corrected or annotated, other authorized holders of the information are notified about the correction or annotation and that all copies of the information in the possession of the CBSA are corrected / annotated.

8.3 ☒ AND, if appropriate, ensure that the "Privacy Notice" or "Consent Statement" and the relevant **PIB** are amended to identify the data-matching activity including the source(s).

NO

8.4 ☐

Explain why such measures will not be adopted: *(This information is mandatory)*

9. Use of Personal Information

Use of the EDL information is governed by four facets: CBSA's legislative authority to collect and use the personal information; the MOU between the CBSA and each of the participating provinces and, importantly, by the notice provided to the applicant at the point when they applied for the EDL and via the particular PIB registered by the CBSA and published in Info Source.

- 9.1 ☒ Implement controls and procedures to ensure that access to the personal information for such purposes will be limited to authorized individuals who need to know the information to perform their official duties. *(Identify the work positions within the program or activity that have a valid reason to access and handle the personal information, and limit access to individuals occupying those positions.)*
- 9.2 ☒ AND, ensure that the "Data Flow Diagram" or "Data Flow Tables" completed for "Section 4 – Flow of Personal Information" of the CBSA PIA identify the areas, groups and individuals (e.g., the positions) within the CBSA who have a need-to-know to access to or handle the personal information, including their geographical location and where the personal information will be stored or retained. *(See Section IV of Appendix "C" of Directive on Privacy Impact Assessment for a list of elements that must be included in the data flow diagram or data flow tables.)*
- 9.3 ☐ AND, if the purposes for which the personal information is used includes any use(s) of the information for a non-administrative purpose, (such as research, statistical, audit and evaluation purposes) the CBSA will adhere to the requirements and principles in the **CBSA Privacy Protocol For Non-Administrative Purposes** (2012), in accordance with section 6.2.15 of the *Policy on Privacy Protection*, to address any impact that such non-administrative uses may have on privacy.
- 9.4 ☐ Identify below any other uses of the personal information, in other words, any routine uses that are not directly related to the purpose of the collection, or, which are not consistent with that purpose or for which the information was disclosed to the CBSA pursuant to subsection 8(2) of the *Privacy Act*:
-
- 9.5 ☐ AND, ensure that these other uses are reflected in the relevant **PIB**. (In accordance with subsection 9(1) of the *Privacy Act*, if these other uses are not described in the PIB in CBSA Info Source, the CBSA is required to record each use on the individual's file. Describing them in the PIB is, therefore, a far more efficient practice – see Question 11.)
- 9.6 ☐ AND, include a description of these other uses in the "Privacy Notice" or "Consent Statement", as appropriate,
- ☐ AND, ensure the all the other applicable requirements listed under "YES" at Question 9 are met.

10. Disclosures Directly Related to the Administration of the Program or Activity

Will personal information be disclosed for purposes directly related to the administration of the program or activity? (This includes, for example, disclosures to other programs within the CBSA, other federal institutions, other governments, international organizations, private sector organizations or individuals.)

YES

- 10.1 ☐ Please check all applicable boxes below and, for each disclosure, identify the name of the organization or third party to which personal information will be disclosed. If it is disclosed within the CBSA, please identify the branch and the program or activity.
- 10.1.1 ☒ Within the CBSA for another program or activity

Detail : *Enforcement / Intelligence within the context of Lost/Stolen/Fraudulently Issued Documents*

10.1.2 ☐ Other federal government institutions

Detail :

10.1.3 ☐ Provincial, territorial or municipal governments institutions

Detail :

10.1.4 ☐ Foreign government institutions and entities thereof

Detail :

10.1.5 ☐ International organizations

Detail :

10.1.6 ☐ The private sector (e.g., contractor or other external service provider)

Detail :

10.1.7 ☐ Other

Detail :

10.2 ☒ AND, ensure that:

- a) any such disclosure is made in compliance with section 8 of the *Privacy Act*, which allows disclosures of personal information with consent of the individual to whom the information relates (subsection 8(1)) or without consent in certain and limited circumstances pursuant to subsection 8(2) of the Act;
- b) only personal information elements that are necessary for the intended purpose are disclosed;
- c) the organization or third party receiving the personal information is authorized to do so;
- d) administrative, physical and technical safeguards appropriate to the sensitivity of the information will be applied to protect the information during and after its transmission (see Question 15);
- e) the organization or third party to which the personal information will be disclosed for the administration of the program or activity are identified in the "Consistent Use" section in the relevant **PIB** in *CBSA Info Source*, including the specific purpose of the disclosure; the "**Privacy Notice**" or "**Consent Statement**" describes any disclosures of information; (For a copy of the CBSA Privacy Notice and Consent Statement template, contact the ATI and Privacy Division) and,
- f) the "Data Flow Diagram" or "Data Flow Tables" completed in "*Section 4 – Flow of Personal Information*" of the CBSA PIA include details on the disclosed personal information: (See Section IV of Appendix "C" of *Directive on Privacy Impact Assessment* for a list of elements that must be included in the data flow diagram or data flow tables.)

10.3 ☒ AND, any disclosure of personal information to another federal institution or outside the

Government of Canada is governed by a formal agreement or arrangement (e.g., a Memorandum of Understanding, an accord, a contractual arrangement, etc.) to ensure that appropriate privacy protection clauses are included, and, where applicable, include provisions for inter-jurisdictional or transborder flows of personal information. Such clauses must cover the following topics:

- a) Control over personal information, where appropriate.
- b) Limitations on the collection, retention, use and disclosure of personal information.
- c) Measures (administrative, technical and physical) to protect the integrity and confidentiality of personal information.
- d) Measures governing the disposition of the personal information, where relevant
- e) Measures to ensure or verify that the personal information is only used for the purposes related to the agreement, arrangement or contract.
- f) Obligations are to be extended to other parties such as subcontractors.

11. Accounting For New Uses or Disclosures Not Reported in CBSA Info Source

Will controls and procedures be implemented to account for any new use or disclosure of the personal information that is not included in the relevant PIB published in CBSA Info Source?

YES

11.1 ☒ Appropriate controls and procedures have been or will be implemented to ensure that:

- a) the head of the institution (The ATI and Privacy Director) or the appropriate delegate is notified about any new use or disclosure of personal information that is not reflected in the PIB description published in *CBSA Info Source*;
- b) the consent of the individual to whom the information relates is obtained in writing, as appropriate, prior to any new use of the information for an administrative purpose that is not reflected in the relevant PIB published in *CBSA Info Source*, unless the new use is considered to be consistent with the purpose for which the personal information was obtained or compiled and the Privacy Commissioner is notified, by the CBSA ATI and Privacy Director, forthwith regarding the new consistent use;
- c) except as permitted under subsection 8(2) of the *Privacy Act*, any disclosure of personal information for a purpose that is not reflected in the relevant PIB published in *CBSA Info Source* will only be made with the consent of the individual to whom the information relates;
- d) a record is kept for any new use or disclosure of personal information not described in the relevant PIB published in *CBSA Info Source*, and that this record is stored with the personal information to which it relates and retained for a minimum period of two years following such a use or disclosure; *(The record of use or disclosure should include the name and title of the person authorizing the use or disclosure; the name of the institution, person, organization or body receiving the information; a description of the use or purpose of disclosure; a copy of the information disclosed, or a description in sufficient detail to allow a determination of exactly what information was used or disclosed.)*
- e) if the information is disclosed to a federal investigative body under paragraph 8(2)(e) of the *Privacy Act*, the record of disclosure will be kept in a separate PIB for a period of two years where it will be available to the Privacy Commissioner for review upon request; *(e.g., Standard PIB*

"Disclosure to Investigative Bodies" PSE 913)

- f) the Privacy Commissioner is notified, by the CBSA ATI and Privacy Director, forthwith, as required under subsection 9(4) of the Act, of any new use or disclosure that is consistent with the purpose for which the information was obtained or compiled, but which is not reflected in the relevant **PIB** published in *CBSA Info Source*;
- g) the relevant **PIB** is amended in time for the next edition of *CBSA Info Source* to include any new use(s) or disclosure(s) that are consistent with the purpose for which the information was obtained or compiled, as well as any routine use(s) or disclosure(s) that do not fall within the categories of purpose of collection or consistent use (e.g., these would include disclosures of the information under subsection 8(2) of the Act that take place on a regular basis. By including these routine uses or disclosures in the PIB, the CBSA would be relieved from the obligation to record each use or disclosure on the individual's file); and
- h) the Privacy Commissioner is notified, by the ATI and Privacy Director, prior to or forthwith, as required under subsection 8(5) of the Act, about any disclosures made or to be made in the public interest or in the interest of the individual to whom the information relates.
- i) Other

Detail : *(This information is mandatory)*

12. Safeguards - Statement of Sensitivity

Has a Statement of Sensitivity (SoS) or similar analysis been completed to assess the degree of sensitivity of the personal information to be collected and retained for the program or activity? (Input to this section should be coordinated with and reviewed by the CBSA – IT - Security Directorate)

Statutory reference: Sections 7 and 8 of *Privacy Act*.

Policy reference: Appendix C of *Directive on Privacy Impact Assessment* and sections 6.2.17 to 6.2.21 of *Directive on Privacy Practices, Policy on Government Security, Operational Security Standard: Management of Information Technology Security (MITS)*

YES

- 12.1 ☐ The information contained in the SoS or similar analysis has been taken into account when assessing the level of risks to privacy in "Section 2 - Risk Area Identification and Categorization" of the CBSA PIA.

NO

- 12.2 ☒ Please explain why a SoS or similar analysis was not considered necessary to assess the sensitivity of the information.

Detail: The 2015 Statement of Sensitivity "Traveller Admissibility Determination Support Service" is considered sufficiently broad as to include the expansion of the EDL program to allow CBSA BSO's access to the EDL database.

13. Safeguards - Threat and Risk Assessment

Has a Threat and Risk Assessment (TRA) or a similar security assessment been completed for the program or activity? (Input to this section must be coordinated with and reviewed by CBSA – IT - Security Directorate)

YES

- 13.1 ☒ Reference the title of the TRA or other security assessment in "Section 7 – Supplementary Documents List" and provide a brief synopsis of the assessment in the space below:

Detail: CBSA IT Security IT Security impacted the components of the release to integrate RFID readers into conventional passage lanes at POEs via a Consultation Report. On all elements, the view across all risks being evaluated was LOW. A TRA for the RFID Processor to allow the CBSA to read additional RFID-enabled documents including the Canadian EDLs is in progress. At this time, the completion date is unknown.

- 13.2 ☐ AND, obtain assurances from the officials responsible for the program or activity that the measures recommended in the assessment have been implemented to ensure the confidentiality, availability and integrity of the personal information.
- 13.3 ☐ AND, ensure that any residual risks to personal information are known and accepted by the executive or senior official responsible for the program or activity and the Head or delegated authority for the *Privacy Act*. (ATI and Privacy Director)

NO

- 13.4 ☐ If a TRA or similar security assessment is underway, simply reference that fact in the space below and indicate when it is likely to be completed. If there is no intent to complete one, please explain.

Detail : (This information is mandatory)

14. Safeguards - Administrative, Physical and Technical

Please identify below any administrative, physical and technical safeguards in place, or to be implemented, for this program or activity to ensure the confidentiality, availability and integrity of the personal information. (Safeguards must be commensurate with the sensitivity of the information, the risks identified, and the nature of the media in which the information is stored, handled and transmitted. This section must be completed with input from CBSA – IT - Security Directorate)

Statutory reference: Sections 7 and 8 of *Privacy Act*

Policy reference: Appendix C of *Directive on Privacy Impact Assessment* and sections 6.2.17 to 6.2.21 of *Directive on Privacy Practices, Policy on Government Security, Operational Security Standard: Management of Information Technology Security (MITS)*

Please check all that apply, including safeguards identified by the TRA or similar security assessment.

14.1 Administrative safeguards

- ☒ Internal security and privacy policies and procedures
- ☒ Staff training on privacy and the protection of personal information

- ☒ Screening and security checks of employees
- ☒ Appropriate security levels for employees who will have access to personal information
- ☒ Contingency plans and documented procedures in place to identify and respond to security and privacy breaches, and to communicate security violations to the data subject, law enforcement authorities and relevant program managers
- ☒ Regular monitoring of users' security practices
- ☒ Methods to ensure that only authorized personnel who need to know have access to personal information
- ☐ Other

Detail : The above will be addressed by the TRA to be completed as referenced in 13.1

14.2 Physical safeguards

- ☒ Restricted access areas
- ☒ Security guards
- ☒ Identification badges are worn by staff at all times
- ☒ After hours alarms and monitoring systems
- ☐ Locked filing cabinets
- ☐ Combination locks
- ☐ Safes
- ☐ Cipher locks
- ☒ Key cards
- ☐ Video surveillance (closed-circuit television)
- ☒ Secured server locations
- ☒ Backups secured off-site
- ☐ Other

Detail :

14.3 Technical safeguards

- ☒ Role-based user authorization and authentication
- ☐ Biometrics
- ☒ Passwords (minimum of 6 characters long, include alpha and numeric characters)
- ☒ Passwords are changed by users every 90 days and recently used passwords cannot be re-used)
- ☒ Password protected screensavers
- ☒ Session-time out security (automatically locks an account after a session has been idle for a specified amount of time)
- ☒ Firewalls
- ☒ Intrusion Detection System (IDS)
- ☐ Virtual Private Network (VPN)

- ☒ Encryption of sensitive information
- ☒ Government of Canada Public Key Infrastructure Certificates (PKI)
- ☐ External Certificate Authority (CA)
- ☒ Audit trails
- ☐ Other

Detail :

15. Technology and Privacy - Tracking Technologies

Will the information system(s) used to deliver the program or activity employ cookies or other tracking technologies to collect personal information about users and their transactions? (Input to this section should be coordinated with and reviewed by the CBSA – IT - Security Directorate)

Statutory reference: Sections 4 to 10 of the Privacy Act and section 4 of Privacy Regulations

Policy reference: Subsections 6.1.1, 6.1.3, 6.1.9, 6.2.9 to 6.2.13, 6.2.17 and 6.2.23 of Directive on Privacy Practices

YES

- 15.1 ☐ The specific tracking technologies to be used is adequately described under Part 6: Technology and Privacy of "Section 2 – Risk Area Identification and Categorization" of the CBSA PIA
- 15.2 ☐ AND, the collection of any personal information using such technologies is reflected in the relevant **PIB** and in "Section 3 – Analysis of Personal Information Elements" of the CBSA PIA;
- 15.3 ☐ AND, the use of such technologies to collect information about users and their transactions is adequately reflected in the "**Privacy Notice**";
- 15.4 ☐ AND, those responsible for implementing and using tracking technologies to collect personal information or who may have access to personal information collected through these methods are made aware of privacy and security policy requirements;
- 15.5 ☐ AND, where personal information collected through such tracking technologies is used to make a decision that directly affects the individual to whom the information relates, it will be retained for a minimum of two years after the last administrative action as required under the *Privacy Regulations*.

NO

- 15.6 ☒ Tracking technologies are not used to collect personal information about users.

16. Technology and Privacy - Surveillance or Monitoring

Will the new or modified program or activity result in new or increased surveillance or monitoring of a targeted population? (Input to this section should be coordinated with and reviewed by the CBSA – IT -

Security Directorate)

Statutory reference: Sections 4 to 10 of *Privacy Act*, section 4 of *Privacy Regulations* and section 8 of the *Charter of Rights and Freedoms*

Policy reference: Subsections 6.1.1, 6.1.9, 6.2.9 to 6.2.13 and 6.2.17 of *Directive on Privacy Practices*

YES

- 16.1 ☐ Consult with your legal advisors to determine whether or not such surveillance or monitoring activities raise any issues relating to the *Charter of Rights and Freedoms*, the *Privacy Act* or other applicable acts.
- 16.2 ☐ And, ensure the surveillance or monitoring method(s) to be used, the characteristic(s) of the targeted population and the scope of the surveillance or monitoring are adequately described under Part 6: Technology and Privacy of "*Section 2 – Risk Area Identification and Categorization*" of the CBSA PIA.
- 16.3 ☐ AND, any personal information collected or created as a result of such surveillance or monitoring is described in the relevant **PIB** and in *Section 3 – Analysis of Personal Information Elements* of the CBSA PIA.
- 16.4 ☐ AND, the collection or use of personal information through surveillance or monitoring is adequately reflected in the "**Privacy Notice**", unless such notification might result in the collection of inaccurate information or defeat the purpose or prejudice the use for which the personal information is collected.
- ☐ If notice about surveillance or monitoring will not be provided

Detail explain why: *(This information is mandatory)*

- 16.5 ☐ AND, those responsible for implementing and using such surveillance or monitoring method(s) or who may have access to personal information collected or created through these methods are made aware of privacy and security policy requirements.

NO

- 16.6 ☒ The new or modified program or activity will not result in surveillance or monitoring.

While the CBSA will not use the RFID technology for surveillance or monitoring, EDL applicants are informed about the risks of RFID in the Applicant Guides.

Ontario's EDL Applicant's Guide states,

A Radio Frequency Identification (RFID) chip is embedded into the card. The chip, which is not visible, contains a unique identification number only and does not contain any personal information. At the U.S. port of entry, an RFID reader will retrieve this reference number and transmit it to the U.S. Customs and Border Protection network, when the traveller attempts to enter into the U.S. Data encryption, secure networks and firewalls protect the information while it is being transmitted. U.S. Customs and Border Protection (CBP) uses the reference number to query the Ontario EDL records securely stored in Canada by the Canada Border Services Agency (CBSA). CBSA retrieves the record and securely sends the information to CBP to help determine the holder's identity and potential admissibility into the United States.

A protective sleeve is provided with your EDL card to help shield your personal Radio Frequency

Identification (RFID) number. It is recommended that you always keep your EDL card inside the sleeve and only remove it when you are using it at U.S. or Canadian ports of entry or if asked by any police officer to show your driver's licence.

Manitoba's EDL Applicant Guide states,

Radio frequency identification, or RFID, is a generic term for technologies that use radio waves to automatically identify objects. There are several methods of identification, but the most common is to store a number that identifies an object on a microchip that is attached to an antenna (the chip and the antenna together are called an RFID transponder or an RFID tag). The antenna enables the chip to transmit the identification number to a scanner when it is polled. The scanner converts the radio waves reflected back from the RFID tag into digital information that can then be passed on to computers that can make use of it. Each Manitoba EDL or EIC has a RFID chip embedded in it to help speed up processing when you arrive at United States border crossings with RFID scanners. As you approach the border at a land or water port of entry into the United States, an RFID scanner will read your unique identifier number in your card's RFID chip (called the RFID Tag Value) at a maximum distance of 4.5 metres. The United States border agent can then use your unique identifier number to quickly retrieve the personal information about you stored in a secure database that he or she needs in order to verify your identity and citizenship and to help determine whether or not you will be allowed to enter the United States.

It is important to note that the RFID chip contains one piece of personal information — the RFID Tag Value that points to your EDL or EIC record. EDL and EIC records for all provinces issuing the cards are kept in a secure database located in Canada and maintained by the Canada Border Services Agency (CBSA). To deter and detect fraudulent EDLs and EICs, your RFID chip is engraved with a Tag Identifier (TID) that uniquely identifies each RFID chip and prevents cloning. Your EDL or EIC card is manufactured utilizing multiple layers of the highest quality plastics making it counterfeit resistant. It will also withstand ultraviolet (UV) rays and will not fade with age.

If there are no RFID scanners at the border crossing where you are entering the United States, the border agent can swipe the MRZ on the back of your EDL or EIC to access your unique Encoded Document Number. Your Encoded Document Number performs the same function as the RFID Tag Value — allowing the border agent to quickly access personal information about you from your EDL or EIC record in the CBSA's secure, Canadian database — but the actual numbers of the RFID Tag Value and Encoded Document Number are different for added security. Your EDL or EIC will come with a protective sleeve to help prevent tracking of your movements by an unintended RFID scanner. It is essential for your privacy protection that you keep your EDL or EIC in this sleeve to block the ability that any RFID scanner would have to read the chip on your card without your knowledge.

However, if your RFID chip is read by an unintended scanner, the scanner would be able to retrieve the RFID Tag Value only; that number could not be used to access your personal information stored on the secure CBSA database.

Your personal information is safely transmitted from the secure CBSA database through a secure encrypted network connection to the United States Border Crossing Information (BCI) system. Manitoba EDLs and EICs are also mailed in a protective envelope to prevent any possibility of the RFID chip being read during delivery to the cardholder. It is important that your protective sleeve is not torn or otherwise damaged as it could potentially allow reading of the card by an unintended scanner. If the protective sleeve becomes damaged, immediately obtain a replacement sleeve free of charge from an Autopac agent or any Manitoba Public Insurance Service Centre.

British Columbia's EDL Applicant Guide states,

Radio Frequency Identification Chip:

The EDL contains a Radio Frequency Identification (RFID) chip. The only information on the RFID chip is a unique identifier number and a tag ID number.

Unique identifier number:

RFID readers are located at select U.S. border entry locations. The RFID reader will read the unique identifier number, which will be used by U.S. customs to access limited personal information that's stored in a secure database located in Canada and maintained by the Canada Border Services Agency.

Your information will then appear on the U.S. customs officer's screen as you approach the booth. If there are no RFID readers at the border crossing, the optical character recognition (OCR) unique identifier number on the back of your EDL will call up the same information from the same Canadian database when you present your EDL card to the U.S. customs officer at the booth.

Tag ID number:

The tag ID number is embedded in the RFID chip by the chip manufacturer making it very difficult, if not impossible, to clone a copy of your card. Neither of these numbers are your driver's licence number and there is no other information on the RFID chip.

Protecting your EDL:

There are some situations in which a person with access to RFID-reading technology may be able to read your unique identifier numbers from a short distance, without your knowledge. Even if your unique identifiers are read, your personal information is safe from unauthorized access as it's protected in a secure CBSA database. The numbers on the RFID don't relate to any other personal identifiers such as your driver's licence number and can't be used to impersonate you.

For added security, ICBC provides a protective sleeve for your EDL to prevent the RFID chip from being read when you're not using it to cross the border. You'll receive the protective sleeve in the mail with your card. For your protection keep your EDL in the sleeve when it's not being used and replace it if it becomes torn or crumpled. Replacement sleeves are available at ICBC driver licensing offices without charge for EDL cardholders.

17. Considerations Related to Compliance, Regulatory Investigation, Enforcement

Does the program or activity involve compliance/regulatory investigation or law enforcement, surveillance or intelligence gathering that targets specific individuals against whom penalties, criminal charges or sanctions may be applicable?

Statutory reference: Sections 4 to 10 of *Privacy Act*, section 4 of *Privacy Regulations* and section 8 of the *Charter of Rights and Freedoms*

Policy reference: Subsections 6.1.1, 6.1.9, 6.2.9 to 6.2.13 and 6.2.17 of *Directive on Privacy Practices*

YES

- 17.1 ☒ Consult with your legal advisors to determine whether or not the compliance/regulatory investigation or law enforcement activities raise any issues relating to the *Charter of Rights and Freedoms*, the *Privacy Act* or other applicable acts.
- 17.2 ☒ AND, identify the legislative authority and the specific regulatory or law enforcement purpose involved:

Detail: Personal information is collected pursuant to the *Customs Act*, the *Immigration and*

Refugee Protection Act (IRPA), the Customs Tariff, the Excise Act, the Excise Tax Act the Export & Import Permits Act, the Controlled Drugs and Substances Act (CDSA) and the Proceeds of Crime (Money Laundering) & Terrorist Financing Act for the purposes of obtaining information on persons who are suspected of border related illegal activities, including contraband smuggling and immigration violations.

- 17.3 ☒ AND, if the legislative authority differs from the legal authority for the program or activity, ensure it is adequately reflected in the response to Question 1 of "Section 5 – Privacy Compliance Analysis" and in "Section 1 – Overview and PIA Initiation" of the CBSA PIA.
- 17.4 ☐ AND, any personal information collected or created as a result of such regulatory or criminal enforcement, surveillance or intelligence gathering program or activity is described in the relevant **PIB** and in "Section 3 – Analysis of Personal Information Elements" of the CBSA PIA.
- 17.5 ☐ AND, the collection or use of personal information through these compliance / regulatory investigation or enforcement activities is adequately reflected in the "Privacy Notice", unless such notification might result in the collection of inaccurate information or defeat the purpose, or prejudice the use, for which the personal information is collected.
- ☐ If notice about the compliance/regulatory investigation or law enforcement activities will not be provided.

Details: This is an indirect collection of information; no notice is required by law however two of the provinces already notify individuals that the information could be used for the enforcement of IRPA.

NO

- 17.6 ☐ The program or activity does not involve the conduct of regulatory or criminal enforcement, surveillance or intelligence gathering.

SECTION 6 - Summary of Analysis and Recommendations

- 1) **The Notice provided by the Provinces will need to be Updated** – Currently, the notice provided by Ontario and British Columbia informs applicants that the CBSA may use the information for the administration and enforcement of the *Immigration and Refugee Protection Act*. It is unclear how that would apply to Canadian citizens and the provinces should consider updating their notice provisions to the simple language from the MOU: CBSA will use the information for border crossing purposes. Manitoba does not inform applicants of the current proposed use. If it is determined that the administration and enforcement of IRPA is sufficient notice for applicants, then the CBSA would be permitted to use the EDL information for Ontario and BC card holders only. Manitoba does not provide notice of that use of the information and is clear in communicating the permissible uses. While the option of “consistent use” has been considered, it is likely that the use of the information would be considered a secondary use and, as such, would require the consent of current Manitoba cardholders. If it is determined that the administration and enforcement of the *Immigration and Refugee Protection Act* cannot be applied to Canadian citizens crossing the border, then the use of all information related to current card holders would be considered a secondary use and, as such, would require the consent of all current card holders.

Mitigation Measure – The CBSA is using this information for immigration purposes, which is a primary use under IRPA. Ontario and Manitoba have advised the CBSA that notifications have been drafted to send to existing cardholders to reflect the expanded use of the data by the CBSA. The CBSA has strongly encouraged British Columbia to issue a similar notice. At the time of this PIA, those notices are still being drafted.

- 2) **The MOUs with the Provinces should be updated** – The MOUs as originally drafted with the provinces did not contemplate the CBSA using the EDL information for border crossing purposes.

Mitigation Measure – The MOUs with each of the provinces have been amended to ensure the language for permissible uses is inclusive of the CBSA's accessing of the data held on behalf of the provinces.

- 3) **The Personal Information Bank needs to be updated:** Suggested revisions to the Personal Information Bank are included as part of this PIA.

Mitigation Measure – In summary, the description was updated to reflect a description of the personal information, not the program. Elements of personal information collected were updated to be comprehensive. The Purpose in the PIB was updated to reflect a new use of the information by the CBSA BSOs. The legal authorities were updated to include references to IRPA. Availability of the information for query by the U.S. was removed from consistent uses, as this had been the primary use for the collection.

- 4) **There is no demonstrated notice provided at the border by BSOs** – There are no Privacy Notice scripts provided to BSOs for use at land / water POEs.

Mitigation Measure – the provision of notice when a BSO collects border crossing documents (Passport, Birth Certificate or EDL) and notes the border crossing details should be considered for

implementation by the CBSA. This risk and mitigation measure, however, is not limited to the EDL initiative.

- 5) **An EDL not in its protective sleeve could be read by the CBSA** – A traveller wishing to use another document for entry could trigger an inadvertent collection of EDL data by not having the EDL in its sleeve.

Mitigation Measure – to address this scenario, the BSO has the ability to “flush” the travel document in the course of processing the traveller. The passage history would not reflect the EDL.

- 6) **No TRA has been completed for the RFID Processor, which will allow the CBSA to read RFID-enabled documents including the Canadian EDLs** – A threat and risk assessment verifying the risks associated with reading RFID-enabled documents has not yet been completed.

Mitigation Measure – to address this, the CBSA is in the process of completing a TRA. The completion date is not yet known; however, the process has been started.

- 7) **The installation of the RFID readers, including the construction of the required infrastructure, has begun** – given the lack of a TRA supporting the usage of RFID technology, the risk to personal information has not yet been assessed.

Mitigation Measure - to address this, the CBSA is in the process of completing a TRA. The completion date is not yet known; however, the process has been started.

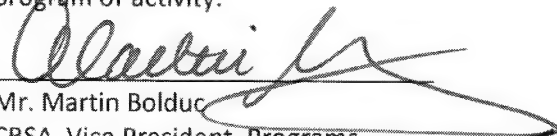
SECTION 7 - SUPPLEMENTARY DOCUMENTS LIST

- Privacy Impact Assessment of the Enhanced Driver's Licence (EDL) Program, January 2008
- Enhanced Driver's Licence and Enhanced Identification Card Program Privacy Impact Assessment Update, December 2008
- Ontario Enhanced Driver's Licence Applicant Guide
- Manitoba Enhanced Driver's Licence Applicant Guide
- British Columbia Enhanced Driver's Licence Applicant Guide
- Memorandum of Understanding Respecting the development and implementation of Ontario's Enhanced Driver's Licence and Enhanced Photo Card Program between the Government of Canada and Province of Ontario
- Memorandum of Understanding Respecting the development and implementation of the Manitoba Enhanced Identification Card and Enhanced Driver's Licence Program between the Government of Canada and the Government of Manitoba
- Memorandum of Understanding Respecting the development and implementation of British Columbia's Enhanced Driver's Licence and Enhanced Identification Card Program between the Government of Canada and the Province of British Columbia
- Addendum to the *Memorandum of Understanding Respecting the development and implementation of Ontario's Enhanced Driver's Licence and Enhanced Photo Card Program*
- Addendum to the *Memorandum of Understanding respecting the development and implementation of the Manitoba Enhanced Identification Card and Enhanced Driver's Licence Program*

-
- Addendum to the *Memorandum of Understanding Respecting the development and implementation of British Columbia's Enhanced Driver's Licence and Enhanced Identification Card Program*
 - Secondary Processing and Passage History IT Threat and Risk Assessment (TRA)


SECTION 8 - FORMAL APPROVAL

The following signature represents a commitment to comply with sections 4 to 8 of the *Privacy Act* and the related privacy policy requirements outlined in the CBSA PIA as they relate to the administration of the identified program or activity.


Mr. Martin Bolduc
CBSA, Vice President, Programs

21/07/2017
Date

The following signature represents a commitment by the Head of the institution or his/her delegate(s) who is responsible for establishing personal information banks in accordance with section 10 of the *Privacy Act*.


Mr. Dan Proulx
CBSA Access to Information and Privacy Director

JUL 18 2017
Date

Annex A: Privacy Compliance Checklist and Other Considerations

Note: The table below must be used to keep an account of actions completed and to track outstanding actions required to achieve privacy compliance:

Privacy Compliance Analysis question #	Action required to support legal and policy compliance (cross reference to relevant question of <i>Section 5 – Privacy Compliance Analysis</i>)	Done	To be done
1	Legal authority for the program or activity has been established and is reflected in the relevant PIB.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2	a) The categories and elements of personal information to be collected for the new program or activity have been carefully assessed based, for example, on the CBSA's experience gained with the administration of a similar program or activity. The personal data collected will be limited to only that which is required.)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	b) Categories and elements of personal information have been described in the relevant PIB for the program or activity.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	c) Controls and procedures will be implemented to ensure the CBSA does not collect more personal information than necessary for the program or activity and that a continuing need exists for the personal information and its collection.	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Use of Enhanced Driver's Licence and Enhanced Identification Card Information by the Canada Border Services Agency

PIA

Privacy Compliance Analysis question #	Action required to support legal and policy compliance (cross reference to relevant question of <i>Section 5 – Privacy Compliance Analysis</i>)	Done	To be done
4 and 5	<p>a) All of the requisite "Privacy Notices" and "Consent Statements" that meet the requirements of sections 6.2.9 to 6.2.12 of the <i>Directive on Privacy Practices</i> have been drafted. (Texts of the notices and consent statements must be included as an annex.) For a copy of the CBSA Privacy Notice and Consent Statement template, contact the ATI and Privacy Division.</p> <p>b) Controls and procedures have been implemented to keep records of individual consents, and to ensure that persons acting on behalf of individuals who do not have the capacity to provide consent have the authority to do so under section 10 of the <i>Privacy Regulations</i>.</p>	<input checked="" type="checkbox"/>	<input type="checkbox"/>
7	<p>a) A Records Disposal Authority (RDA) has been approved by Library and Archives Canada to authorize the disposal of the records containing personal information for the program.</p> <p>b) Controls and procedures have been implemented within the program or activity and the CBSA ATI and Privacy Division to ensure that information that has been used for an administrative purpose will be kept for the minimum retention period established by the Privacy Regulations.</p> <p>c) Reference to the RDA, the retention period and the disposition standards for the program have been cited in the relevant PIB.</p>	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
8	Controls and procedures are in the process of being implemented to ensure that the personal information associated with the program is as accurate, complete and up-to-date as necessary.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Other Privacy Considerations related to specific principles that are not explored in the previous 17 sections: (these considerations should be explored in the Executive Summary)			
Openness	Describe how the results of any privacy impact assessment or audit will be made available to the public. The Executive Summary will be published on the external CBSA ATI and Privacy Division website at http://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/pia-efvp/atip-airp/pias-sefp-eng.html	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Are policies and practices relating to the proposal's management and handling of personal information available to the public?	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Is there a communications plan to explain to the public how personal information will be managed and protected?	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Use of Enhanced Driver's Licence and Enhanced Identification Card Information by the Canada Border Services Agency		PIA	
Privacy Compliance Analysis question #	Action required to support legal and policy compliance (cross reference to relevant question of <i>Section 5 – Privacy Compliance Analysis</i>)	Done	To be done
Individual's Access to Personal Information	Is there a clearly defined and easy process for individuals to access such information and/or communicate with appropriate individuals with respect to policies and practices relating to management and protection of personal information?	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Where appropriate, will public consultation take place on the privacy implications of the proposal?	<input type="checkbox"/> N/A	<input type="checkbox"/>
	Is the system designed to ensure that an individual can have access to his/her personal information, including all other programs or applications that have received copies of the information? s. 12(1)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Challenging Compliance	Are there documented procedures developed or planned on how to make privacy requests or requests for the correction of personal information? s. 12 (2)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Are individuals provided with access to their personal information in the official language of their choice? s. 17(2)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	If appropriate, are individuals provided with access to their personal information in an alternative format? s. 17(3)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Are the complaint procedures for the proposed program or service consistent with legislated requirements? s. 29-35	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	To improve information management practices and standards, has a procedure been established to log and periodically review the nature, frequency and resolution of complaints?	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Are there oversight and review mechanisms implemented or available to ensure accountability?	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Have oversight agencies, including the Office of the Privacy Commissioner, issued reports or opinions on issues that would be relevant to the proposal?	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Annex B: Office of the Privacy Commissioner Expectations

In their March 2011 document, *Expectations: A Guide for Submitting Privacy Impact Assessments to the Office of the Privacy Commissioner of Canada*, the Office of the Privacy Commissioner (OPC) has expressed the importance of analysing the risks of the project, program or initiative against the ten universal privacy and fair information practice principles of the Canadian Standards Association Model Code for the Protection of Personal Information.

The most relevant demonstration of the privacy risk and compliance analysis is the action plan. The OPC has said the following in their **Expectations** guide with respect to the action plan:

Once privacy risks and their proposed mitigating measures have been identified, we expect to see an Action Plan drawn up by the institution, indicating a specific time frame for remedying or mitigating the risks that have been identified, and if possible, naming a specific person or staff position accountable for taking action.

The action plan must list all privacy risks and compliance issues identified in the PIA and supplementary documentation. All risks and issues must be organized by the 10 universal privacy principles.

All recommendations and proposed mitigation strategies must also be described in the action plan. Identify the responsible program area and the timeline for completion or implementation of the strategy. The ATI and Privacy Division will provide programs with an action plan template to be addressed near the end of the PIA process.

The expectations of the OPC for each privacy principles are included below for your reference.

Accountability

Under this principle the OPC would expect to see documentation of an administrative structure for privacy, including input from legal services, access to information and privacy and information technology branches within an institution, with defined processes for determining when new projects require PIAs, for carrying them out, implementing mitigating measures and auditing for assurance of compliance. We expect PIA reports to be signed off at the appropriate level, and that training in privacy issues and procedures has been documented and is refreshed with employees regularly; and that privacy protective language is included in all contracts with third parties handling personal information in accordance with TBS guidance documents and internationally accepted best practices; and that regularly scheduled privacy compliance audits will be undertaken and the findings acted upon.

Identifying Purposes

The *Privacy Act* restricts federal government institutions to the collection of personal information that relates directly to an operating program or activity of the institution, so we would expect to see a clear description of the program and why each piece of information is needed; a description of the legislative authority for the collection; a clear listing of all the data elements collected; copies of any relevant documents such as application forms identifying the purpose for the collection or on-line notices of use; a copy of an up to date Personal Information Bank (PIB) description; a statement of any proposed new consistent use of information previously collected and a clear rationale as to how the use is reasonable and directly connected to the original collection -- this may include an analysis of how an individual to

whom it relates would reasonably expect it to be used for that purpose; a statement outlining any intended secondary uses of the information; whether the information is collected directly from the individual and if not, why; and a description of how personal information used for planning, forecasting or statistical purposes would be anonymized or de-linked from individual identifying information.

Consent

This is closely tied to the Identifying Purpose principle. Under this principle, OPC would expect to see a copy of notification language on forms or websites; a clear description of the purpose for collection; a rationale for not seeking consent, as is provided for in the *Privacy Act*; for web sites, a copy of the Privacy Notice Statement under which personal information is submitted to the institution.

Limiting Collection

Under this principle, OPC would expect to see a clear justification of the need for each data element collected, in keeping with the requirement of the *Privacy Act* that no personal information is to be collected by a government institution unless it relates directly to an operating program or activity of the institution; an indication that a data minimization exercise has been undertaken to ensure that each data element is necessary and that this exercise will be refreshed regularly; and that information collected from another department for a secondary use will be purged of all but the essential data elements before use.

Limiting Use, Disclosure and Retention

Under this principle, OPC would expect to see a description of the specific uses and proposed disclosures of the information; a clear statement limiting the use of the information to the purposes identified; a clear retention policy and disposition schedule that is also noted in the PIB; a process for destruction of the information that is in keeping with the *Privacy Act* and Regulations; copies of MOUs or agreements with third parties to whom information is disclosed governing its use, retention and disclosure, and clauses with contractors or sub-processors of information indicating the originating institution has the right to audit for compliance with privacy provisions.

Accuracy

Under this principle, OPC would expect to see a description of the process used by entities to ensure accuracy, particularly when administrative decisions are made; a description of how changes to records are logged and monitored; a statement of whether automated decision-making based on risk profiles is being undertaken and how automated decisions are vetted for accuracy; an explanation of the processes open to individuals seeking to correct information; a description of the process by which second or third parties to whom information has been disclosed will be notified of changes and corrections to the record; and a description of how audit trails of records transactions are monitored and evaluated.

Safeguards

OPC would expect to see under this principle a description of the physical and electronic safeguards that are in place to protect information; a Threat & Risk Assessment (TRA) with emphasis on privacy risks and concerns and a discussion of how these concerns have been remedied or addressed; a notation that encryption is used for personal information both in transit and at rest; a description of how system logs of information transactions are monitored for inappropriate use, including viewing of the information; strong electronic access control, including controls on remote access, and the use of mobile devices; policies for the use of portable storage devices such as flash drives; a description of role-based access

controls; and a description of the steps taken to ensure complete destruction of the information at the end of its life cycle.

Openness

Under this principle, OPC would expect to see a summary of the PIA written in plain, understandable language, posted on the institutional website in a manner accessible to the general public and containing a link to the relevant PIB description in CBSA Info Source; for particularly sensitive or privacy invasive programs we would expect to see the public communications plan described in the PIA, including a variety of methods such as posters, brochures and media announcements as well as detailed discussion of the PIA in the institution's Annual Report under the *Privacy Act*; a description of consultations with key stakeholders and the privacy risks or concerns raised should be readily available on the website; the name and contact information of an individual accountable for the handling of personal information should be easily obtained through the website or by calling the institution's main public number.

Individual Access

Under this principle, OPC would expect the PIA to include a description of any informal process the CBSA may have in place for access to and correction of personal information; an up to date and comprehensive description of information contained in the PIB corresponding to the initiative; a description of the process by which information in the hands of third parties is corrected following requests; a description of how the general public is made aware of these processes, for example, by a link and/or a toll-free number shown on the home page of the institutional website.

Challenging Compliance

OPC would expect to see the PIA address this principle by indicating clearly who is responsible for receiving and resolving privacy complaints; describing complaints that may have been received in any similar activity or pilot project and how they were handled; including privacy issues in project evaluations or feasibility reports; describing how and when compliance audits for privacy will be undertaken; including information on how to file a complaint with OPC under the *Privacy Act*; and reporting in some detail on specific and/or systemic privacy issues in its Annual Reports.

Annex C: Categories of Personal Information

The **Description** section in a personal information bank (PIB) describes the personal information in the records to which the bank relates. Treasury Board Secretariat has established the following categories of personal information, which give examples of specific elements of personal information that fall under each category. The purpose of the categories is to reduce the number of personal information elements that need to be listed in the Description section. These categories are representative of the personal information collected by most institutions, and they now appear in many of the CBSA registered PIBs. The ATI and Privacy Division modified the original list to reflect CBSA business lines.

- Biographical information (e.g. work history, curriculum vitae, family information, Passenger Information, etc.)
- Biometric information (e.g. blood type, eye or facial scan, DNA, finger / hand prints, etc.)
- Contact information (e.g. work and / or home information, including postal and e-mail addresses, telephone, fax, cell phone numbers, etc.)
- Citizenship status or Nationality (e.g. citizen, landed immigrant, etc.)
- Crew detailed information
- Criminal checks / history (e.g. information related to criminal record checks, investigations, charges, conviction dates and locations, pardons, etc.)
- Date of birth
- Date of death
- Destination City
- Employee identification number (e.g. Personal Record Identifier)
- Employee personnel information (e.g. records of attendance and leave, notices of disciplinary action, alternative work arrangements, decisions concerning compensation and fitness for work, official languages qualifications, salary, deductions, level of security clearance, performance reviews and appraisals, rating board assessments, including evaluation notes from staffing boards, training and development course applications and evaluations, etc.)
- E-Ticket Information
- Financial information (e.g. income, investments, mortgages, loans, orders of garnishment, financial institution information for direct deposit and other banking purposes, including name and branch number of institution, account number(s) and name(s) on accounts, etc.)
- FOSS ID / GCMS UCI / IBAS Ref #
- Gender
- Itinerary Cities
- Language (e.g. mother tongue, official and other languages, etc.)
- Medical information (e.g. psychological assessments, blood type, etc.)
- Name (e.g. last name (surname/family name), given names (first, second or more), maiden name, nicknames, aliases, etc.)
- Opinion or views of, or about, individuals
- Passenger Name
- Passport Number or Travel Document Number
- Place of ticket purchase

Photos

Physical attributes (e.g. height, weight, color of hair and eyes, physical markings (scars, tattoos, body piercing), etc.)

Place of birth

Place of death

Port of Embarkation and Port of Debarkation

Signature

Special Travelling Considerations such as Employee Pass, Buddy Pass and Parental Passes

Visa Number



Faces on the Move: Multi-camera Screening

Privacy Impact Assessment (PIA)

Traveller Programs Directorate
Programs Branch
January 14, 2016

PROTECTED B

The image shows the word "Canada" in a serif font, with a small Canadian flag to its right. The background of the footer is a dark, textured image of a maple leaf.

Table of Contents

EXECUTIVE SUMMARY	4
ABBREVIATIONS AND ACRONYMS	8
DEFINITIONS	10
SECTION 1 – INTRODUCTION	12
A. Background/Overview	12
B. DRDC and CSSP	12
C. CBSA Proposal and Project	13
D. Project Roles and Responsibilities	14
E. Overview of the Technology Demonstration	15
F. Post-Demonstration Analysis and Report to DRDC	18
G. Goals of the Project	18
H. Scope of the PIA	18
SECTION 2 – OVERVIEW AND INITIATION	20
SECTION 3 – FOUR-PART TEST	26
SECTION 4 – RISK AREA IDENTIFICATION AND CATEGORIZATION	30
A. Type of Program or Activity	30
B. Type of Personal Information Involved and Context	31
C. Program or Activity Partners and Private Sector Involvement	33
D. Duration of the Program or Activity	34
E. Program Population	34
F. Technology and Privacy	35
G. Personal Information Transmission	38
H. Risk Impact to the Institution	39
I. Risk Impact to the Individual or Employee	40
SECTION 5 – ANALYSIS OF PERSONAL INFORMATION ELEMENTS	41
SECTION 6 - FLOW OF PERSONAL INFORMATION	43
Example of a Data Flow Model - Table	54
Internal Use and Disclosure	55
External Use and Disclosure	55
Retention / Storage	56
Other Possible Considerations	57
SECTION 7 - PRIVACY COMPLIANCE ANALYSIS	59
Legal Authority for Collection of Personal Information	59
Necessity to Collect Personal Information	59
Authority for the Collection, Use or Disclosure of the Social Insurance Number	60
Direct Collection - Notification and Consent (as appropriate)	61
Indirect Collection - Consent or Authority under Sec. 10 of Privacy Regulations	62
Indirect Collection - Without Notification and Consent	62
Retention and Disposal of Personal Information	63
Accuracy of Personal Information	64
Use of Personal Information	66
Disclosures Directly Related to the Administration of the Program or Activity	67
Accounting for New Uses or Disclosures Not Reported in Info Source	69
Safeguards – Statement of Sensitivity	70

PROTECTED B

Faces on the Move: Multi-camera Screening

PIA

Safeguards - Threat and Risk Assessment.....	70
Safeguards - Administrative, Physical and Technical	71
Technology and Privacy - Tracking Technologies.....	73
Technology and Privacy - Surveillance or Monitoring	73
Considerations Related to Compliance, Regulatory Investigation, Enforcement.....	74
SECTION 8 - SUMMARY OF ANALYSIS AND RECOMMENDATIONS	77
SECTION 9 - SUPPLEMENTARY DOCUMENTS LIST.....	86
SECTION 10 - FORMAL APPROVAL	87

EXECUTIVE SUMMARY

This privacy impact assessment (PIA) is intended to assess privacy risks within the Canada Border Services Agency's (CBSA's) planned demonstration of facial recognition (FR) technology at Pearson International Airport, currently expected to begin in early 2016. This project is divided into two phases. The demonstration phase will last for six months and will use facial recognition technology to match travellers against a database of previously deported persons (hereinafter referred as the "Previous Deportation Database" or PDD). This will be followed by a three- to six-month lab evaluation phase where the technology's performance will be assessed. Currently, the CBSA has no definitive plans to deploy this technology for full-time operational use. The solution described in the PIA is a demonstration to test the efficacy of FR software in an operational border context. The success or failure of the project will assist CBSA senior management in making further testing decisions regarding FR technology use within the border context. The CBSA recognizes that any future testing or use of FR technology will require an additional PIA.

This PIA has been drafted using the CBSA *Policy on the Overt Use of Audio-Video Monitoring and Recording Technology (AV Policy)* and the *Policy on the Use of Wireless Technology*, as well as the associated Directives, the *Privacy Act* and the *Privacy Regulations*, and the *Immigration and Refugee Protection Act (IRPA)* as references. This PIA addresses only the *Faces on the Move* project, which is completely separate from the CBSA's existing use of Overt Audio/Video surveillance. The *AV Policy* was implemented on August 15, 2011, revised in November 2012, and updated again in July 2013. The current version the policy dates to November 2013. No audio will be collected or used in this project.

The CBSA has identified thousands of international travellers who have been denied entry to Canada or who have been deported after being admitted into Canada. These travellers have been deemed inadmissible for any of a number of reasons, such as security, criminality, health grounds, misrepresentation, or non-compliance with the IRPA. Many of these inadmissible travellers try repeatedly to re-enter Canada. The CBSA uses a list containing the names of previously deported persons and other, similar lists to identify inadmissible travellers at ports of entry (POEs). Many such travellers, however, use false identity documents, or even legally change their names in their home countries and obtain new, legal travel documents under their new names. Name-based lists such as those currently in use have inherent limitations which can be overcome using biometric technologies.

Although FR technology is widely available for a variety of applications, the use of face recognition with live video has not yet been tested in an operational environment by a Canadian law enforcement body. The CBSA is planning to conduct this demonstration of FR technology to assess whether this technology solution is effective, feasible, and accurate for identifying inadmissible travellers in a busy Port of Entry environment.

The CBSA plans to deploy multiple project-specific cameras in the CBSA-controlled area of the international arrivals section of Terminal 3 at Pearson International Airport. The cameras for this project will not be connected to the existing camera network that supports video surveillance at Terminal 3. Also, the project cameras are connected to the project's FR server and associated applications, but not existing CBSA information systems.

Areas and activities that may be monitored or recorded include, but are not limited to: approaches to the arrivals hall, approaches to Primary Inspection Line (PIL) booths, during PIL interviews, approaches

travellers seeking admission into Canada as they move through the CBSA-controlled area. This technology will not be used in Customs Controlled Areas outside the CBSA's traditional processes.

These cameras will record and store images of travellers' faces. No audio will be collected or used in the FOTM project. A dedicated FR system will compare these "live-capture" images with a database of stored images of persons who have previously been deported or removed from Canada that is specific to this technology demonstration. The system will notify CBSA officers when a match is detected. After human review of the match, an officer will be dispatched to find the traveller to refer them to secondary inspection. Some cameras, known as "scene cameras", will also record video of the areas under surveillance. These video recordings will show what a traveller is wearing and carrying and who they are with; this will make it easier for the CBSA to identify and find the traveller in the airport if the traveller is matched by the system with a person of interest.

As the CBSA has no guarantees that a PDD individual will enter through Terminal 3 during the project, volunteer CBSA employees (defined as "actors" throughout this document) will have their photographs and fictitious bio-data elements stored in the FR system as well.

After six months of operation, the equipment will be re-located from Terminal 3 to the CBSA's Science and Engineering Directorate (SED) lab in Ottawa, where further tests will be conducted to measure and possibly improve the system's performance.

Protecting your Personal Information

In order to carry out its mandate, the CBSA must collect a wide variety of personal information. The collection of this information is required in order for CBSA officers to make admissibility decisions regarding persons who wish to enter Canada. Although the CBSA is already using overt video surveillance, this technology demonstration will involve putting that information to a new use that supports the CBSA's admissibility determination processes. The differences between the current AV program and the *Faces on the Move* demonstration are in the ways the information will be used and the length of time it will be retained.

Through the use of closed-circuit television (CCTV) technologies, as described in the *PIA on the Overt Use of Video Monitoring and Recording Technology* that was submitted to the Office of the Privacy Commissioner (OPC) in November 2013, the CBSA is capturing the physical images of travellers or members of the public (although these images are not currently being used to support admissibility decisions), in addition to the other elements of personal information already collected. Within the CBSA, only those employees who require access to video recordings or photographs as part of their duties are permitted to do so as per CBSA policies and procedures.

Some personal information collected through the *Faces on the Move* demonstration may be used in support of the CBSA's admissibility determination process. As a result, photographic and video records (excluding FR templates and related data) may be disclosed internally to CBSA personnel. Within the context of this time-limited technology demonstration, photographic and video records will *not* be shared with any external stakeholders.

Any access to or disclosure of facial photos, scene camera recordings, or PDD records will be governed by the provisions of the *AV Policy*.

Retention

The retention practices for the *Faces on the Move* demonstration will be governed by the provisions of the *AV Policy*, with some variances. In particular, facial photographs, some scene camera recordings, and PDD records must be retained until the end of the project. All records will be destroyed at the end of the project, except for records that were used for an "administrative purpose" (e.g., where a match was verified and a traveller was identified and diverted to secondary screening). Any records used for an administrative purpose will be retained for two years following the date of last use in accordance with s. 4 of the *Privacy Regulations*.

Right of Access

All records, regardless of storage medium, will be stored either in a locked cabinet (container or a safe) or in a secure room designed in accordance with specifications approved by the Infrastructure and Information Security Division of CBSA.

Records will be securely retained in accordance with established policies and guidelines, and may be disclosed within the CBSA. For the duration of this time-limited technology demonstration, records will not be shared with external organizations.

Individuals may formally request access to their personal information, or access to corporate records related to or created as a result of the *Faces on the Move* project by contacting the Access to Information and Privacy (ATIP) Division. More information about this can be found at: <http://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/pia-efvp/atip-aiprp/menu-eng.html>. In addition to the requirements specified on the Treasury Board of Canada Secretariat Personal Information Request form, individuals requesting information described by this bank must provide the subject and date of correspondence, incident and location and legal authority for those acting on behalf of an account holder or estate.

Accountability

If individuals have concerns about the collection, use, disclosure or retention of their personal information, they may issue a complaint to the CBSA ATIP Division. Complaints should be made in writing, and include their name, contact information, and a brief description of their concerns. Contact information for the ATIP Division at the CBSA can be found here:

<http://cbsa-asfc.gc.ca/agency-agence/reports-rapports/pia-efvp/atip-aiprp/contact-eng.html>

To make a compliment, comment or complaint, the CBSA has made available a feedback form to help us to understand our clients and improve the delivery of our programs and services. Information on providing feedback can be found here:

<http://www.cbsa-asfc.gc.ca/contact/com-eng.html>

The CBSA posted a Video Recording and Monitoring Privacy Notice on its external website on November 19, 2012. This Privacy Notice states:

Privacy Notice**Video Monitoring and Recording**

The Canada Border Services Agency (CBSA) uses video monitoring and recording technology to fulfill its mandate and to increase its ability to protect the public, and to protect employees and assets of the Agency. The use of video monitoring and recording technology is an integral part of the CBSA's security framework and operations management.

Cameras monitor and record CBSA operations at ports of entry and inland offices. Areas and activities that may be monitored or recorded include, but are not limited to: primary interviews, secondary examinations, interactions at CBSA information counters, cashier counters, commercial counters, detention cells, and interview rooms. Cameras may also monitor the movement of travellers and goods from one point in a CBSA operation to another, for example, from primary to secondary.

Use of Recordings

The CBSA collects personal information using overt video monitoring and recording technologies at ports of entry and inland CBSA service locations, to carry out the mandate of the CBSA under the authority of the Canada Border Services Agency Act. Recordings may be used to investigate suspected offences related to border legislation, and may be used as evidence in court proceedings. Recordings may also be disclosed as permitted by legislation to the Canadian Security Intelligence Service, the Royal Canadian Mounted Police, and/or to municipal, provincial or local law enforcement agencies to investigate or enforce federal laws.

Retention and Disposal

Any new or replacement video monitoring and recording equipment must be able to retain recordings for no less than 30 days. Recordings that are used by the CBSA shall be kept for two (2) years following the date of their last use.

Upon expiry of the above retention periods, recordings are permanently deleted/overwritten, or in the case of removable media, recordings are physically destroyed.

Access to Information

Individuals have the right to access their personal information and the right to ensure their personal information is appropriately protected under the Privacy Act. The information collected is described in Info Source under the Overt Audio-Video Surveillance Personal Information Bank CBSA PPU 1104.

ABBREVIATIONS AND ACRONYMS

The following is a list of abbreviations and acronyms used in this report:

ATIP	Access to Information and Privacy (Division of CBSA)
AV	audio-video
<i>AV Policy</i>	<i>Policy on the Overt Use of Audio-Video Monitoring and Recording Technology</i>
CA	certificate authority
CAF	Canadian Armed Forces
CBSA	Canada Border Services Agency
CCTV	closed-circuit television
CD	compact disc
CoP	Community of Practice
CPIC	Canadian Police Information Center
CSIS	Canadian Security Intelligence Service
CSS	Centre for Security Science
CSSP	Canadian Safety and Security Program
DFD	data flow diagram
DND	Department of National Defence
DRDC	Defence Research and Development Canada
DVD	digital video disc / digital versatile disc
FOSS	Field Operations Support System
FOTM	Faces on the Move
FR	Facial Recognition
GCMS	Global Case Management System
HR	Human Resources
I	identification
IDS	intrusion detection system
IEEE	Institute of Electrical and Electronics Engineers
IRB	Immigration and Refugee Board
<i>IRPA</i>	<i>Immigration and Refugee Protection Act</i>
ISTB	Information, Science and Technology Branch
MIDA	Multi-Institutional Disposition Authorities
<i>MITS</i>	<i>Operational Security Standard: Management of Information Technology Security</i>
MOU	Memorandum of Understanding

PROTECTED B

Faces on the Move: Multi-camera Screening

PIA

N/A	not applicable
NCMS	National Case Management System
OPC	Office of the Privacy Commissioner
PAA	program activity architecture
PDP	Previous Deportation Database
PIA	privacy impact assessment
PIB	personal information bank
PIL	Primary Inspection Line
PKI	public key infrastructure
POC	Privacy Oversight Committee
POE	port of entry
PSC	Public Safety Canada
RCMP	Royal Canadian Mounted Police
RDA	Records Disposition Authority
RFID	radio frequency identification
SED	Science and Engineering Directorate
SIN	social insurance number
SoS	statement of sensitivity
TBS	Treasury Board of Canada Secretariat
TC	Transport Canada
TRA	threat and risk assessment
USB	universal serial bus
VPN	virtual private network
Wi-Fi	A trademarked term that identifies wireless networking products that comply with the IEEE 802.11 standards

DEFINITIONS

This section provides definitions of the terms frequently used in this report:

Administrative purpose	The <i>Privacy Act</i> defines an “administrative purpose” to be the use of an individual’s personal information in a decision-making process that directly affects that individual.
Consistent use	Is a use that has a reasonable and direct connection to the original purpose(s) for which the information was obtained or compiled. This means that the original purpose and the proposed purpose are so closely related that the individual would expect that the information would be used for the consistent purpose, even if the use is not spelled out.
Facial recognition	As used in this report, is the technologies and processes used to identify a person by comparing a digital image or video frame of the person’s face with a database of known facial images.
Info Source	Is a series of annual Treasury Board Secretariat publications in which government institutions are required to describe their institutions, program responsibilities and information holdings, including PIBs and classes of personal information. The descriptions are to contain sufficient clarity and detail to facilitate the exercise of the right of access under the <i>Privacy Act</i> . Data-matching activities, use of the SIN and all activities for which privacy impact assessments were conducted have to be cited in <i>Info Source</i> PIBs, as applicable. The <i>Info Source</i> publications also provide contact information for government institutions as well as summaries of court cases and statistics on access requests.
Personal Information Bank	Is a description of personal information that is organized and retrievable by a person’s name or by an identifying number, symbol or other particular assigned only to that person. The personal information described in the personal information bank has been used, is being used, or is available for an administrative purpose and is under the control of a government institution.
Primary Inspection Line	The term “Primary Inspection Line” is used to refer to the point at which the person entering Canada makes a report of his or her person and goods as required under the <i>Customs Act</i> and the IRPA. The CBSA has PIL booths from which officers conduct primary examinations.
Scene camera	A video camera deployed as part of the <i>Faces on the Move</i> project that records wide-angle video scenes at various locations in the CBSA-controlled areas of Terminal 3 at Pearson International Airport. When a potential match from the Previous Deportation Database is identified, a short video clip from a scene camera will be added to the match record. The video clip will be centred in time and space on the matched facial image. It will show the larger context of the potentially matched traveller by showing what the traveller is wearing and carrying and the people around the traveller.
Transitory Record	As defined by Library and Archives Canada and for the purposes of this policy are those records that have no enduring value to the CBSA. They are records that are required only for a limited time to ensure the completion of a routine action or the preparation of a subsequent record but do not include records that are required to control, support or document the delivery of programs, to carry out operations, to

PROTECTED B

Faces on the Move: Multi-camera Screening

PIA

Previous Deportation
 Database

make decisions, or to account for activities of government. (Source: MIDA 2.1, 4. Definition)

A database of selected previously deported persons created specifically for the *Faces on the Move* project. The database will contain facial images and related biographical information (e.g., name, date of birth, warnings) extracted from the CBSA's existing Previously Deported Persons list. The database will contain entries for persons who have been deemed highly likely to attempt to return to Canada during the *Faces on the Move* demonstration.

SECTION 1 – INTRODUCTION

This section below provides an overview of the project. It is supported by the remaining sections of this PIA and is intended to ensure a description of the project is clear at the onset of reviewing this document.

A. Background/Overview

In 2014, the Canadian Border Services Agency (CBSA) received funding from the Defence Research and Development Canada (DRDC) for a project that will test the readiness of facial recognition (FR) technology as a means of screening against a database in an operational environment. This Privacy Impact Assessment (PIA) provides the background on the project, its partners, the test period (herein referred to as the “demonstration period”), the evaluation period, and the associated privacy risks. The project is called *Faces on the Move (FOTM)*.

B. DRDC and CSSP¹

As an agency of Canada’s Department of National Defence (DND), the DRDC provides DND, the Canadian Armed Forces (CAF) and other government departments as well as public safety and national security communities the knowledge and technological advantage needed to defend and protect Canada’s interests at home and abroad.

In 2012, the DRDC established the Canadian Safety and Security Program (CSSP), which aims to invest in science and technology projects that will strengthen Canada’s ability to anticipate, prevent, mitigate, prepare for, respond to, and recover from natural disasters, serious accidents, crime, and terrorism. The CSSP is led by DRDC’s Centre for Security Science (CSS), in partnership with Public Safety Canada (PSC) and uses a collaborative model that gathers the best minds from government, industry, academia, response and emergency management agencies, and international organizations to work on the most pressing safety and security issues facing Canadians.

That collaborative model extends to the manner in which the CSSP/DRDC provides funding for various types of projects, which must meet CSSP requirements identified through risk and vulnerability assessments and are associated with the priorities established by the CSSP; one of which is border and transportation security. CSSP-funded projects allow public safety and security professionals to work with science and technology experts to identify challenges, develop knowledge and tools, and provide advice that will help protect Canada, its people, and institutions. Currently, the CSSP funds approximately 200 projects and activities which are led by either federal, provincial, territorial and municipal governments, or academic institutions, through federal contracting mechanisms managed by Public Works and Government Services Canada.

One of the funding avenues for the CSSP is the Call for Proposal process which invites all levels of government, industry, and academia to submit project proposals for innovative science and technology solutions to address identified risks, vulnerabilities, and gaps in public safety and security capabilities. In the spirit of the CSSP’s collaborative framework, proposals often team up private sector expertise with government programs to address a specific issue. Upon approval by the DRDC of a proposal, the lead

¹ This section was adapted from multiple sections of the DRDC website found here: <http://www.drdc-rddc.gc.ca/en/index.page>.

organization is able to use the DRDC funds to hire its partners (identified in their proposal) to assist in project delivery.

C. CBSA Proposal and Project

In 2013, the CBSA submitted a proposal to the DRDC/CSSP via the Call for Proposal process to seek funding to test FR technology within a border context. The proposal included the following private sector and academia partners:

- Face 4 Systems (formerly known as NextGenID)
- ADGA Group Consultants Inc.
- Université du Québec – Montréal (specifically the École de Technologie Supérieure - ÉTS)

In 2014, based on the CBSA proposal, the DRDC awarded funds to the CBSA to assist in the testing of FR technology. In-kind funding by the CBSA through the use of employee resources, project management, and technical expertise was needed to ensure the project budget was appropriate.

Within the CBSA, the Information, Science and Technology Branch (ISTB), and specifically the Science and Engineering Directorate (SED), will lead the project in consultation with Programs Branch and Operations Branch. The Traveller Program Directorate is the Programs Branch sponsor and, in part, is the approving authority for this PIA. ISTB has led a working group consisting of working-level representatives from the following areas to ensure broad consultation and awareness of the project:

- Comptrollership (Security and Professional Standards)
- Corporate Affairs (Communications and ATIP Policy & Governance)
- Border Operations
- Enforcement and Intelligence Operations
- ISTB
- Traveller Program Directorate
- Traveller Program Transformation
- Greater Toronto Area Region (location of the demonstration – Pearson Airport)

The purpose of the project is to demonstrate the readiness of FR technology for potential screening applications. The CBSA anticipates the technology could assist in overcoming some of the limitations of name-based lists. Specifically, it can assist in identifying travellers who are known to be inadmissible who seek to enter Canada using false identity documents or documents issued under different names.

The demonstration period will begin in early 2016 (for period of six months) at Terminal 3, Toronto Pearson International Airport (YYZ). In order to demonstrate the solution, additional cameras will be installed and configured before the beginning of the six month-long demonstration period. In addition to camera installation, a secure server, workstation equipment, handheld devices, and software will also be installed. The cameras and associated wiring will operate separately from the existing CCTV network within the terminal and will be positioned and utilized in accordance with the CBSA's *Policy on the Overt Use of Audio-Video Monitoring and Recording Technology*; it is noted that only images and video are captured by the project-specific cameras and audio will not be captured or used.

D. Project Roles and Responsibilities

The funding provided by the DRDC allows for the CBSA to procure the services and products of the partners identified in the proposal. Therefore, once the DRDC approved the funding, the CBSA was able to sole-source hardware, software, and consulting services from the proposal partners. In that regard, the following provides an overview of the roles and responsibilities of partners and stakeholders in this project:

1. Defence Research and Development Canada (DRDC)
 The *FOTM* project is managed by the DRDC's CSS with CBSA's SED providing the project management function. The DRDC provides oversight to ensure its funding is used appropriately.
2. CBSA Science and Engineering Directorate (SED)
 SED, a directorate under ISTB, will manage the project, coordinate all entities of the project, and is responsible for internal reporting (CBSA senior management) and external reporting (DRDC). The funds provided by the DRDC require quarterly reports as well as a final report which the SED is responsible for producing. From an IT Project Management perspective SED is the Project Authority and the Technical Authority.
3. Face4 Systems (formerly NextGenID)
 Face4 Systems is a Canadian-based (Ottawa) company which designs, develops, deploys and supports FR security products, services and solutions for government and private organizations around the world. Face4 Systems' products focus on live face capture and face image quality analysis and processing. The company is a value added re-seller of FR software made by Cognitec, which is headquartered in Dresden, Germany with satellite offices in the U.S., Australia, and Canada. For this project, Face4 Systems will provide the following:
 - Purchasing cameras, server, desktop workstation (for BSO Adjudicator) and the handheld devices (For BSO Rover)
 - Installation and removal of the above products
 - Training on the products
 - Component testing of the products
 - Technical support
 - Assist in evaluating the results of the demonstration

Face4 Systems staff will have access to the PDD photos, images and videos taken from the cameras, and other personal information as part of its responsibility to assist in evaluating the demonstration. Access to all personal information will be limited to a CBSA location.

4. Université du Québec (École de Technologie Supérieure (ÉTS))
 Scientists from the ÉTS are not involved during the demonstration period, but will develop the test plan and system assessment methodology for post-demonstration scientific analysis during the evaluation period. After the demonstration, ÉTS staff will analyze performance data (match scores) from the Montreal campus of the University of Quebec. The performance data does not include any personal information.

5. ADGA Group Consultants, Inc.

The ADGA Group is responsible for authoring the PIA for the project. The company and its consultants play no further role in the project.

As part of any CSSP-funded project, there are two additional participants that are best described as passive participants: the Community of Practice (CoP) and an External Advisory Committee.

1. Community of Practice

Communities of Practice (CoPs) are groups of subject matter experts brought together by CSSP who share a common interest in a given area of expertise and work together to facilitate knowledge-sharing and collaboration. CoPs are an essential element of the CSSP, providing access to a rich pool of collective knowledge and experience to support the development of new or enhanced science and technology knowledge and capabilities and to provide advice and guidance in the development of evidence-based policy, decision-making and operational and strategic planning. Members of the CoP may be provided access to regular project updates, the final scientific analysis report, and may be invited by DRDC to attend a final presentation; however, none of the information provided to the CoP contains the personal information of actors or individuals from the PDD.

For this project the CoP includes the following government institutions: Canadian Security Intelligence Service (CSIS), Transport Canada (TC), Royal Canadian Mounted Police (RCMP), and the CBSA.

2. External Advisory Committee

The External Advisory Committee comprises organizations that have expertise or interest in the area of a DRDC-funded project; in this case, biometrics. The Committee meets quarterly and provides the project with feedback on relevant information from the subject area.

For this project, the External Advisor Committee includes: CBSA, RCMP, PSC, TC, Calgary Police, the Office of the Privacy Commissioner of Ontario, and the U.S. Department of Homeland Security. These organizations have had prior experience or involvement in projects related to FR technology. For example, the Ontario Privacy Commissioner has experience with the implementation of FR in Ontario casinos to identify self-reported problem gamblers attempting to enter a casino. Also, the Calgary Police has implemented FR technology to match crime-scene photos to its collection of mug shots.

The Committee is not provided any reports or verbal communication containing the personal information of actors or PDD.

E. Overview of the Technology Demonstration

Section 6 of this PIA provides a detailed explanation of the technology demonstration and how it will be deployed, utilized, and analyzed. The diagram and text that follows is provided as a high level explanation, which supports Section 6.

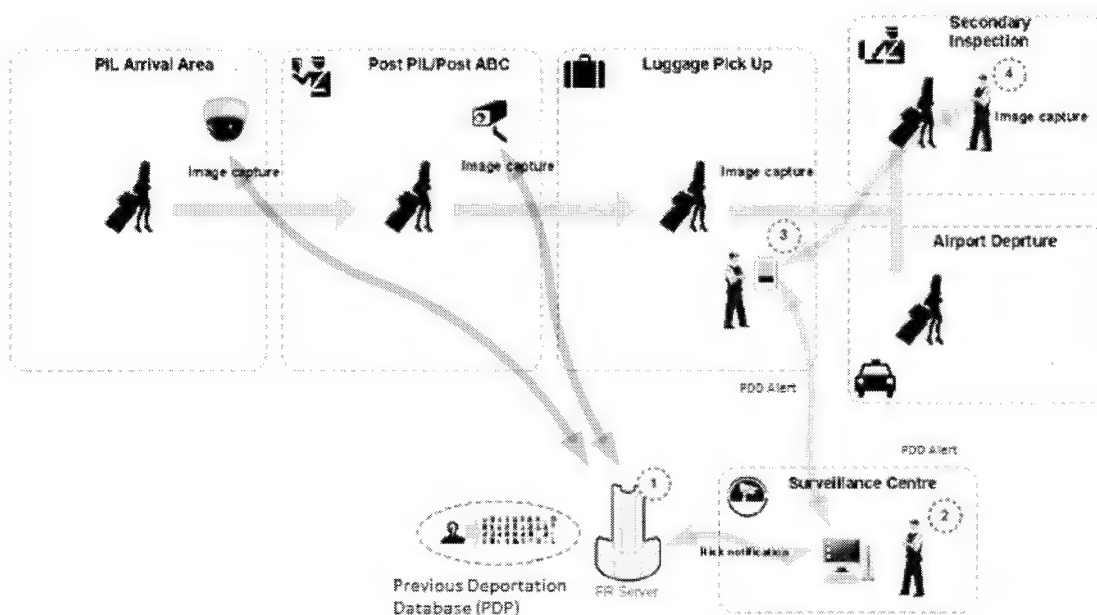


Figure 1: High-level System Overview

1 As part of the project, a dedicated server will be installed with no connection to any CBSA information system or to the existing CCTV network. The server will run the FR software and will be connected to the cameras that will be installed solely for this project. The server will also store personal information on two groups of individuals: the control group, who are actors from among volunteer CBSA employees; and the operational group, which consists of extracts from an existing inventory of Previously Deported Persons maintained within existing CBSA systems. The database that will be uploaded to the server will be limited to 5,000 individuals who have been previously deported and have attempted to return to Canada at least one time in violation of their removal order.

In this first step, the cameras will capture still images and video of individuals entering the CBSA-controlled area at Terminal 3 of Pearson International Airport. The images will be sent to the FR server and matched with the previously uploaded PDD and actors using FR software provided by Face4 Systems.

2 In Step 2, if the FR software identifies any potential matches, it sends a match notification to a Border Security Officer (BSO), identified for the purposes of this project as an “adjudicator”. The dedicated workstation located inside a secure Surveillance Centre will have an application installed locally that receives the possible match notification from the FR server and prompts the adjudicator for a decision. The adjudicator is presented with an image of the match from the PDD and images from the Terminal 3 cameras to make the adjudication decision, as well as a five second video of the individual.

3 If the BSO adjudicator believes a match has occurred, a BSO Rover (BSO patrolling the CBSA-controlled section of the airport) is notified via a project-specific handheld device. Communication between the adjudicator workstation and the Rover BSO handheld device is over a cellular network consistent with the CBSA’s *Policy on the Use of Wireless Technology*. The device will

provide the Rover BSO with an image of the individual, a five-second video taken from the project-specific cameras and data from the PDD (Name, DOB, FOSS ID#, and alerts). The Rover BSO will use this information to locate the individual and validate the adjudicator's match assessment.

4 Assuming the Rover BSO is confident that a match exists, the individual is referred to secondary examination at Terminal 3 where a BSO will assess the individual's identity and admissibility to Canada. Upon escorting the individual to secondary, the Rover BSO will inform the secondary BSO that a FOTM match has occurred. All BSOs working in Terminal 3 are aware of the FOTM demonstration and that any FOTM match requires independent validation using existing systems and procedures for potential matches of the PDD. FOTM procedures for secondary immigration BSOs will clearly state the requirement that any FOTM match requires independent identity validation using existing systems and procedures.

When an operational match results in action being taken with respect to a traveller, such as a referral to secondary examination, the match record, including all PDD information, live-capture photos, and scene video, will be exported to secondary storage (CD, USB, or similar) in accordance with CBSA policies, which require that any interaction with a traveller (i.e., referring the individual for secondary examination based on the FR demonstration) must be kept for two years. The storage device will be kept on the individual's file, so that a permanent record of the information that led to the action can be preserved; however, evidence supporting deportation will be limited to the identity validation efforts of the secondary immigration BSO. If deportation is the result of the secondary examination, then non-FOTM data, including video from existing Terminal 3 cameras, will be used to support the deportation proceeding. Only in rare and extraordinary cases does CBSA envision FOTM data being a supporting piece of information in a deportation proceeding.

For the four-step process outlined above and shown in Figure 1 above, the FR system will be configured to send a match notification to the adjudicator only if a potential match has a high probability of being a true positive match. This will reduce the number of false positives (where the system incorrectly matches a traveller's face with an image from the PDD sent to the BSOs).

F. Post-Demonstration Analysis and Report to DRDC

Once the six-month demonstration period is over, the technology will be removed from the airport for an additional three to six months of evaluation in a lab setting. The project will remove the FR server, cameras, wiring, adjudicator workstation, and the handheld devices. The only potential change to the removal plan is that the project cameras may be provided to the POE and be re-wired as they are no longer valuable to the demonstration after the demonstration period. At the writing of this PIA, a final decision on whether to provide these cameras to the POE had not been made.

Also following the demonstration period, representatives from the CBSA's SED (as the project lead), Face4Systems, and the ÉTS will analyze the demonstration data to scientifically examine the results. Face4 Systems staff will have access to the personal information that was used during the demonstration to determine the effectiveness of the software. Their access to personal information will be restricted to a CBSA location.

Additionally, scientists from the ÉTS will analyze performance data from the demonstration, which will not include any personal information. ÉTS access to the performance data will be performed outside of a CBSA location. ÉTS will be given access only to performance metrics (i.e., match scores) and not to personal information of particular cases/individuals.

G. Goals of the Project

It is critical to this PIA that there is a clear understanding regarding the goal and intent of the project, which is to scientifically test FR software in a border context.

Therefore, the goal of the project is simply to scientifically test the technology. This PIA and the project is not a Pilot Project to test a solution for possible future implementation. There is no underlying plan within the CBSA to implement the FR software after the demonstration. The test results of the solution may support future CBSA decisions on how to further test FR, but the CBSA is clearly in the very early stages of making a decision on whether FR technology can be used effectively in a border context.

As part of the funding provided by the DRDC, the project team is required to write a scientific report on the demonstration and the test results. The report will be made public on the DRDC website and disseminated to project stakeholders. The report may also be reviewed by members of the CoP and the Advisory Committee. It will not contain any personal information.

H. Scope of the PIA

The scope of this PIA is limited to the technology demonstration that is managed by the CBSA's SED and supported by the other CBSA Programs and external organizations as outlined in the previous section of this document. As this is substantially different from how the CBSA uses both video surveillance and biometric technologies, this PIA has been written to ensure the demonstration is considering the privacy implications of the project. By analyzing the privacy principles in conjunction with the demonstration, the CBSA is ensuring privacy and the scientific analysis of the technology are both considered when the Agency makes future decisions regarding FR technology.

This PIA identifies two sets of risks: one that are inherent to the demonstration itself and another that are anticipatory and based on the potential future testing and use of FR technology to identify individuals in CBSA controlled areas. The latter group of risks are advisory in nature and have no bearing on the actual scope of this PIA – the demonstration of the FR technology. Privacy considerations of the “actor” group have not been included in the scope of this PIA because this group consists of volunteer participants and will not be used for an administrative purpose.

The CBSA is committed to ensuring that privacy is strongly considered in relation to the use of audio-video monitoring and recording technology. If any future projects stem from the scientific results of this project, subsequent PIAs will be written to ensure privacy risks and their related mitigation strategies are identified before deployment. The CBSA will also ensure subsequent PIAs provide a detailed description of the scientific results of the current demonstration. Moreover, CBSA ATIP will continue to provide updates to the OPC on various privacy-related projects at the CBSA, including but not limited to, any further use of FR and audio-video monitoring and recording.

SECTION 2 – OVERVIEW AND INITIATION

Government Institution: Canada Border Services Agency

Government Official Responsible for the
Privacy Impact Assessment

Barry Kong, Director, Program
Compliance and Outreach Division, CBSA

Head of the government institution / Delegate
for section 10 of the *Privacy Act*

Dan Proulx, ATIP Director, CBSA

Name of Program or Activity of the Government Institution:

Faces on the Move: Multi-camera Screening

Description of Program or Activity:

Faces on the Move: Multi-camera Screening is a Project under the Canadian Safety and Security Program (CSSP) managed by Defence Research and Development Canada (DRDC). The purpose of the project is to demonstrate the operational readiness of FR technology.

The CBSA will demonstrate FR technology to assess its potential for supporting existing programs as an integral part of its security framework to support its admissibility determination and immigration enforcement processes. The use of FR technologies could support the Enforcement, Facilitated Border, and Conventional Border programs, and could increase the CBSA's ability to meet its mandate and its ability to protect the public and its employees. These potential uses provide the necessary justification for CBSA being involved in the testing project, but the project is only intended to test the effectiveness of a FR-based traveller processing solution and provide a scientific assessment of the technology's readiness level. That assessment will be used by the CBSA, and other members of the CoP, to better enable the Border and Transportation Security Community on the current state of FR technology.

Most cameras deployed for this project will monitor and record still images of travellers' faces in the CBSA-controlled areas of Terminal 3 of Toronto's Pearson International Airport. A smaller number of "scene cameras" will record video of travellers as they pass through this area. Areas or activities where travellers' facial images may be recorded include, but are not necessarily limited to: approaches to the arrivals hall, approaches to PIL booths, during PIL interviews, and the approach to immigration point.

Recorded facial images will be compared automatically to a database of persons of interest to CBSA. No audio will be collected or used in the FOTM project. The database will consist of facial photographs and basic biographical information (name, date of birth, FOSS ID#, and alerts) of actors and from CBSA's existing Previously Deported Persons list. All potential matches that have a high likelihood being a true match between an arriving traveller and a person on the PDD will be adjudicated immediately by a CBSA officer. Potential matches with a low likelihood of being a true match will be reviewed, in bulk, for statistical analysis purposes between one to seven days after the travellers' facial images were recorded. For each potential match, a short video clip (from a scene camera) taken at the same time as the facial photograph will be stored on the FR server dedicated to this project (no connection to any CBSA information system). Verified high-likelihood, real-time matches will be communicated to roving CBSA officers in the airport, who will attempt to find the traveller and ask him or her to report to secondary examination for further discussion. The video clip will aid in identifying the traveller by showing what

the traveller is wearing and carrying. Verified lower-likelihood, non-real-time matches will be analyzed statistically, with an objective of reporting on system performance and limitations.

ADMISSIBILITY DETERMINATION

Through the Admissibility Determination program, the CBSA develops, maintains and administers the policies, regulations, procedures and partnerships that enable border services officers to intercept people that are inadmissible to Canada and to process legitimate people seeking entry into Canada within established service standards.

In the traveller stream, border services officers question people upon arrival to determine if they meet the requirements of applicable legislation and regulations to enter Canada. Border services officers will then make a decision to grant entry or refer a person for further processing (e.g. payment of duties and taxes, issuance of a document), and/or for a physical examination.

IMMIGRATION ENFORCEMENT

The Immigration Enforcement Program determines whether foreign nationals and permanent residents who are or may be inadmissible to Canada are identified and investigated, detained, monitored and/or removed from Canada.

Foreign nationals and permanent residents of Canada believed to be inadmissible are investigated and may have a report written against them by a CBSA inland enforcement officer. Depending on the type of inadmissibility, the merits of the report are reviewed. Subsequent to this review, a removal order may be issued against the foreign national or permanent resident in question. Removal orders issued against refugee claimants are conditional and do not come into force until the claim against the removal order is abandoned, withdrawn or denied by the IRB.

REMOVALS

The Removals Program (a sub-program of Immigration Enforcement) ensures that foreign nationals and permanent residents with an enforceable removal order are removed from Canada. Once a person is removal-ready, an interview is conducted to ensure that a travel document is available and that a pre-removal risk assessment is offered by a CBSA inland enforcement officer. Where a valid travel document is not available, CBSA inland enforcement officers liaise with foreign embassies to secure the required travel documents.

Note: This should align with the program named and described in the institution's Info Source Chapter as required under section 5 of the *Access to Information Act*. For institutions that develop a Program Activity Architecture (PAA) as per the *Management, Resources, and Results Structure Policy*, the institutional Info Source chapter must align with the programs, activities and sub-activities described in the PAA.

Description of the class of records associated with the program or activity:

CBSA BPD 1101

Records include audio/video footage of CBSA operations including primary inspection line (PIL) interviews; secondary examinations; interactions at CBSA information counters, cashier counters, commercial counters, in detention cells, and in interview rooms to record audio statements made under the *Immigration and Refugee Protection Act* (IRPA).

CBSA ENF 135

Records related to the Removals Program which enables the CBSA to remove from Canada

PROTECTED B

Faces on the Move: Multi-camera Screening

PIA

individuals who have contravened the *Immigration and Refugee Protection Act (IRPA)* and who are subject of an enforceable removal order. May include records related to the establishment or use of electronic systems used to administer or manage the program including the Global Case Management System (GCMS) and the National Case Management System (NCMS) and the Canadian Police Information Center (CPIC).

CBSA ENF 137

Information from the enforcement records of persons who have come under examination at a port of entry or an investigation at an inland office. Personal information may include name, address, birth date, country of birth, enforcement action undertaken (i.e. inadmissibility reports, arrest reports, hearing or removal under the *Immigration and Refugee Protection Act (IRPA)*), fingerprints, digital photographs, personal histories of refugee claimants, immigration applications and the date and place of each event in the process.

Class of Record Number: CBSA BPD 1101; TBS Registration: 20110287; Bank Number: CBSA PPU 1104

Class of Record Number: CBSA ENF 135; Bank Number: CBSA PPU 1301

Class of Record Number: CBSA ENF 137; TBS Registration: 005218; Bank Number: PPU 032

☐ Proposal for a New Personal Information Bank

N/A

☐ Proposed new Standard Personal Information Bank

☐ **Proposal to modify an existing Standard Personal Information Bank** - identify Standard PIB number and current description:

N/A

Legal Authority for Program or Activity:

Immigration and Refugee Protection Act

- Sections 15(1), 16(1), 16(1.1), 16(2), 16(2)(a), 16(2)(b), 16(2.1), 16(3), 18(1), and 18(2)

Immigration and Refugee Protection Regulations

- Sections 28, 28(a), 28(b), 28(c), and 28(d)

Note: Prior to proceeding with the assessment it is essential that Parliamentary authority for the relevant program or activity be established. Generally, Parliamentary authority is usually contained in an Act of Parliament or subsequent regulations, or approval of expenditures proposed in the Estimates and authorized by an *Appropriations Act*. If legal authority is unclear consult your Legal Service to determine authority for the program or activity. (See question 1 of **Section V**)

Summary of the project / initiative / change:

The CBSA works to promote the free flow of travellers and goods into and out of Canada, while ensuring that security measures are in place to stop and remove potential threats. Keeping Canada's border open to travel and trade, but closed to criminal activity requires the CBSA to manage border operations effectively.

With a workforce of approximately 14,000 employees, the CBSA provides services at 1,200 points across Canada. The CBSA also administers more than 90 acts, regulations, and international agreements, many on behalf of other federal departments and agencies, the provinces, and the territories. In calendar year 2013, the CBSA processed 99.7 million travellers and 14 million commercial shipments.

The CBSA will demonstrate FR technology to assess its potential to support existing programs as an integral part of its security framework to support its admissibility determination process. The use of FR technology may increase the CBSA's ability to meet its mandate and its ability to determine the admissibility of persons seeking entry to Canada. However, the intent of the FOTM project is to test the solution and assist CBSA senior management in any decisions to further explore FR technology.

Project-specific cameras will monitor and photograph travellers' faces and record video of their overall appearance in the CBSA-controlled areas of Terminal 3 of Pearson International Airport. Areas and activities that may be monitored and photographed include, but are not limited to: approaches to the arrivals hall, approaches to PIL booths, during PIL interviews, approaches to immigration point, and within immigration secondary.

Currently, signage at Terminal 3 includes a bilingual placard that states the following:

"This area is under video surveillance. Recordings may be used and shared in accordance with applicable federal legislation. For more information on the CBSA's use of these recordings, please ask to speak with a supervisor or visit www.cbsa-asfc.gc.ca"

At the CBSA, the location of monitoring and recording signage must adhere to three Agency-developed principles:

1. Signs must be posted anywhere video recording technology is being used (Note that the *Policy on the Overt Use of Audio-Video Monitoring and Recording Technology* places limitations on the use of AV technology).
2. Signs must be posted (in order of preference) in at least one of the following areas: just prior to entry to a CBSA-controlled area; at entry points to a CBSA-controlled area, or as soon as possible after entry to a CBSA-controlled area.

3. Signs must be hung in conspicuous locations to allow travelers a reasonable opportunity to know that the area that they are in, or about to enter, is under surveillance.

FR technology will compare the facial images collected from arriving travellers and compare them with images of persons of interest on the pre-generated PDD. When the FR system finds a potential match between a traveller and a PDD entry, it will attach a short video clip of the traveller (taken by a *FOTM* scene camera). If a potential match has a high likelihood of being true, the FR system will immediately notify a CBSA Border Services Officer (BSO) in the Surveillance Centre. The BSO will manually review the collected image, video, and the PDD image and make a final adjudication as to the accuracy of the match. The BSO will send an alert about the verified match to roving BSOs in the immigration hall using wireless technology. The roving officer will receive the alert via a handheld device provided for this demonstration (this handheld device is unique to the *FOTM* demonstration and will not be used for any other purpose; these devices will be removed at the end of the demonstration). The roving BSO will search for the identified person and, upon finding the person, direct him or her to secondary examination. In secondary examination, existing systems and procedures will be used to process the traveller. BSOs working immigration secondary have been made aware of the *FOTM* demonstration and new procedures require them to validate the identity of the individual separate from the *FOTM* match.

FR could assist the CBSA in ensuring the integrity of the border by capturing information relating to persons who contravene the *Immigration and Refugee Protection Act (IRPA)*. For example, FR could assist in detecting contraventions of the following sections of the act:

- *IRPA* section 15, which grants the CBSA the authority to examine persons applying to enter Canada
- *IRPA* section 16, which requires persons making such applications to respond truthfully to the examination
- *IRPA* section 18, which requires every person seeking to enter Canada to appear for an examination to determine the person's admissibility to Canada

Cameras will not be placed in any area where CBSA business is not conducted, or in any area where there would be a heightened expectation of privacy, such as public or employee washrooms, lunch rooms and locker rooms. Information related to travellers, facility employees (non-CBSA) or other members of the public (transport drivers, flight attendants, brokers clearing goods, etc.) is considered to be personal information as defined in section 3 of the *Privacy Act*. For the purposes of this activity and this PIA, any CBSA employee information captured in facial photographs that relates to the function or the position of the employee is not considered to be personal information, in accordance with paragraph 3(j) of the *Privacy Act*. Any information captured related to an employee that does not specifically relate to his/her function or position will be treated as personal information per section 3 of the *Privacy Act*.

The CBSA recognizes that it has broad authorities to stop, question, search, detain and arrest travellers and seize goods and information in the border context. It further recognizes that, in order to carry out its mandate to ensure the safety and security of the Canadian border, it collects and is entrusted with a wide variety of personal information. The CBSA is committed to adhering to all privacy laws and to ensuring that not only are individuals appropriately notified of any collection of personal information, but that all of the information collected is appropriately protected.

The use of FR technology is a new activity. Use of this technology will be guided by the CBSA's overarching policy on the use, retention, disclosure and disposal of audio and video equipment and recordings. Standard Operating Procedures will be drafted to govern the specifics of the *FOTM* project. The CBSA is conducting this PIA to ensure that the privacy risks associated with using, retaining, disclosing and disposing of personal information collected in the course of demonstrating FR technology are adequately addressed.

This PIA reflects the CBSA's planned use of FR technology at Pearson International Airport beginning in early 2016 for period of six months, during which project personnel will analyze the performance of the technology. This will be followed by a three- to six-month lab evaluation phase where the technology's performance in relation to the information collected during the demonstration will be further assessed. At this time, the CBSA has no plans to deploy FR technology for ongoing operational use, regardless of the performance of the technology in this limited demonstration. The testing results may assist future senior management decision on further exploration of FR at the CBSA, but at this time, there are no definitive plans to implement such technology.

This PIA has been drafted using the *AV Policy* as well as the associated Directives, the *Privacy Act* and the *Privacy Regulations*, and the *Immigration and Refugee Protection Act* as references. The *AV Policy* was implemented on August 15, 2011 and revised in July 2013. No audio will be collected or used in the *FOTM* project. The Agency recognizes that the use of the *AV policy* for traveller processing is a new use which is not currently included in this Policy.

The *FOTM* project is a project of the Canadian Safety and Security Program (CSSP), managed by Defence Research and Development Canada's (DRDC) Centre for Security Science (CSS). The CBSA is the government lead for the project.

SECTION 3 – FOUR-PART TEST

The section provides a discussion related to the scope of this PIA and an assessment against the four-part test.

The CBSA recognizes that the four-part test, in part, requires an assessment as to whether the initiative will be effective in achieving a specific purpose. However, this initiative is unique in that it is not a Pilot Project or a Proof of Concept that is being tested so the tested solution can be modified for future use. Instead, the purpose of this project is to provide a foundational dataset regarding the effectiveness of this technology as a whole. This may be used by the CBSA, or its partners, to inform any future plans to deploy FR technology. This careful approach has been taken in recognition of privacy sensitivities inherent in a FR-based matching program.

The four part assessment below must be read with the understanding that it is limited to the scientific evaluation of an FR technology demonstration and does not apply to the application of FR technology within the CBSA's current traveller processing programs. Any future demonstration or testing of FR will result in a PIA that will draw upon the scientific research garnered from this project and be further assessed against the four-part test.

1. Is the measure demonstrably necessary to meet a specific need?

There are many cases of non-Canadians using false names in attempts to enter Canada illegally.

A report by the PBS television show "Frontline" explored how terrorists use fake identity documents to travel the world. The report focused on Ahmed Ressam, the so-called "Millennium Bomber", who first entered Canada in 1994 using a fake French passport. (see <http://www.pbs.org/wgbh/pages/frontline/shows/trail/etc/fake.html>).

In 1970, Palestinian Mahmoud Mohammad Issa Mohammad was convicted in a Greek court of manslaughter and other charges related to an attack against an Israeli airliner that he participated in. This conviction made him inadmissible to Canada. Yet in 1987, he managed to enter Canada under a false name. It took until 2013 for him to be deported (see <http://www.nanaimodailynews.com/news/palestinian-deported-from-canada-1.177617#>).

A U.S. citizen was a fugitive from American justice when he used a false name to enter Canada in 2008. He was eventually arrested and sentenced for crimes he committed in Canada before being deported back to the United States (see <http://www2.canada.com/saskatoonstarphoenix/news/local/story.html?id=07cf4ad2-5d05-4e65-bf2f-fcebd0188783>).

In 2011, an Iranian man in Canada was ordered deported for the second time after being convicted of people smuggling. He provided false identity documents to smuggle Iranians to various countries, including Canada. He also used false passports to enter Canada in 2008 after being removed in 2007

(see <http://news.nationalpost.com/2011/09/23/canada-orders-deportation-of-iranian-suspected-of-human-smuggling/>).

A judgement was rendered in 2013 against a Portuguese citizen who had been previously deported from Canada five times. On at least one of those occasions, he tried to enter the country using a passport with a false name. In this most recent case, he also used a false passport, although this time the name he was using was on a list (see <http://visalawcanada.blogspot.ca/2013/12/portuguese-national-deported-five-times.html>).

A man who entered Canada as a refugee in 2003 was arrested in 2014 in connection with a 2000 murder in Texas. Although the man claims he is not the person wanted in the murder case, fingerprints and photographs have led authorities to conclude he is the same person. According to the news report at <http://bc.ctvnews.ca/cbsa-arrests-man-in-gruesome-2000-murder-in-texas-1.1765595>, the man may have identity documents with several different names on them.

The examples above are cases that made the news of people using false names to evade the CBSA's name-based lists. The CBSA has statistics showing that, just at Terminal 3 of Pearson International Airport, an average of 16 travellers per year were detected using fraudulent, altered, or borrowed travel documents between April 2011 and March 2014. In other words, these people were using documents to claim they were someone else. There is no estimate available for how many people used such documents and were *not* detected.

2. Is it likely to be effective in meeting that need?

The purpose of the *FOTM* technology demonstration is to assess whether FR technology can be effective in detecting attempts by travellers to Canada to subvert name-based lists through false identity documents. The CBSA is committed to taking a careful and educated approach to exploring and potentially implementing FR technology; in part, the CBSA is committed to ensuring a solution is proven, effective, and can be deployed in a way that respects and protects privacy. That is the reason for this demonstration.

FR has been used in other jurisdictions for similar purposes with some success. A 2011 report explains how Ontario casinos use FR technology to identify self-reported problem gamblers if they try to enter a casino. The same report explains how the Canadian Bankers Association has been using FR since 2008 to investigate debit card fraud. See <http://www.theglobeandmail.com/news/national/time-to-lead/canadian-casinos-banks-police-use-facial-recognition-technology/article590998/>.

In November 2014, the Calgary Police Service announced it was implementing FR technology to match crime-scene photos to its collection of over 300,000 mug shots. It is the first police service in Canada to do so. (see <http://www.cbc.ca/news/canada/calgary/facial-recognition-software-to-aid-calgary-police-in-future-investigations-1.2822592>). The Toronto Police Service is considering similar technology (see http://www.huffingtonpost.ca/2014/11/13/toronto-police-facial-recognition-technology_n_6154200.html).

Law enforcement agencies in the U.S. have used FR to match images extracted from CCTV footage at crime scenes with photo databases (often based on drivers' licence photos) to identify criminals (http://www.washingtonpost.com/business/technology/state-photo-id-databases-become-troves-for-police/2013/06/16/6f014bd4-ced5-11e2-8845-d970ccb04497_story.html?hpid=z1).

FR technology is also being tested and deployed at airports around the world. (See, for example, <http://www.govtech.com/public-safety/Sochi-Airport-Uses-Silicon-Valley-Facial-Recognition-Software.html> (Sochi, Russia), <http://www.biometricupdate.com/201407/brussels-airport-to-introduce-facial-recognition-scanners> (Brussels, Belgium), and <http://www.homelandsecuritynewswire.com/dr20140918-japan-to-adopt-automated-airport-gates-equipped-with-facial-recognition-technology> (Tokyo, Japan))

3. Is the loss of privacy proportional to the need?

The *FOTM* demonstration is being deployed only for testing purposes for a limited time (six months). It targets only those persons who are already under an active removal order and who have previously demonstrated intent to return to Canada, despite having been previously deported multiple times.

The FR demonstration will take place only in CBSA-controlled areas of Terminal 3 at Pearson International Airport for a limited time, estimated at six months. After the demonstration, the technology will be removed from the airport for an additional three to six months of evaluation in a lab setting. Personal information already collected at POEs includes a traveller's name; citizenship(s); country and place of residence; and sex. Travellers must also provide a piece of approved identification, such as a passport or enhanced driver's license. Persons seeking entry to Canada may also be required to provide the following information: address, or address of destination in Canada; date of birth (age); marital status; employment status; criminal history; fingerprints; and, information related to accompanying goods entering Canada, including purchases made abroad. FR technology, in addition to the elements mentioned, also captures the physical image of the traveller, which can assist in identifying individuals seeking entry into Canada who are using false identity documents. In all cases, the CBSA only collects the minimum amount of personal information required to make an admissibility decision.

The loss of privacy is minimal given the lower expectation of privacy in a border crossing context. This was noted in the PIA report on the Overt Use of Video Monitoring and Recording Technology submitted to the OPC in November 2013. The *FOTM* demonstration project represents only a nominal increase in the loss of privacy insofar as no different information is being collected above and beyond the CBSA's current use of CCTV technology. The main difference between CCTV and FR is in the technology being used to process the information. This nominal increase in privacy loss will affect mainly those travellers who try to subvert the admissibility determination process.

The CBSA fulfills its mandate through the administration or enforcement of over 90 Acts and Regulations. As a result the Agency is responsible for numerous and complex programs and operating activities, including deciding on traveller admissibility to Canada. In calendar year 2013, the CBSA provided border-related services for 99.7 million travellers arriving at our land, air, rail and marine ports of entry. There is a significant need to find ways to augment the admissibility determination process with automation that can improve efficiency and effectiveness without sacrificing privacy. The CBSA is testing FR technology to determine whether it can meet this need.

4. Is there a less privacy-invasive way of achieving the same end?

The goal of this project is to demonstrate the effectiveness of FR technology in an airport setting. FR is less invasive than other forms of biometric identification, such as fingerprints or retina scans. There is no need to touch or come into close proximity with a biometric scanning device; cameras can be mounted on walls, ceilings, and other architectural features and capture facial images without inconveniencing the traveller.

In terms of the goal of identifying travellers using false identity documents, the only other way to do FR at this time in a way that would be less privacy-invasive would be to have CBSA officers visually examine every arriving traveller and compare their faces with the PDD. Given that the demonstration PDD will contain thousands of photographs, it could take hours to process each traveller through manual FR. This is obviously a totally impractical approach to traveller identification.

Lastly, the CBSA is always balancing methods of enhancing security while expediting travel and commerce; a balance that is often difficult. If the FR technology proves successful, it may also serve a dual purpose: first, to better identify individuals who are attempting to illegally re-enter Canada; and two, by improving the effectiveness of and efficiency of identifying these individuals, reduce wait times at the Primary Inspection Lane (PIL).

SECTION 4 – RISK AREA IDENTIFICATION AND CATEGORIZATION

For Section 3, please check the appropriate box that describes the level of risk related to your program or activity and provide details as indicated in yellow.

A. Type of Program or Activity	Level of Risk
<p>Program or activity that does NOT involve a decision about an identifiable individual</p> <p>Personal information is used strictly for statistical / research or evaluations including mailing list where no decisions are made that directly have an impact on an identifiable individual.</p> <p>The Directive on PIA applies to administrative use of personal information. The Policy on Privacy Protection requires that government institutions establish an institutional Privacy Protocol for addressing non-administrative uses of personal information.</p>	<input type="checkbox"/> 1
<p>Administration of Programs / Activity and Services</p> <p>Personal information is used to make decisions that directly affect the individual (i.e. determining eligibility for programs including authentication for accessing programs/services, administering program payments, overpayments, or support to clients, issuing or denial of permits/licenses, processing appeals, etc...).</p>	<input type="checkbox"/> 2
<p>Compliance / Regulatory investigations and enforcement</p> <p>Personal information is used for purposes of detecting fraud or investigating possible abuses within programs where the consequences are administrative in nature (i.e., a fine, discontinuation of benefits, audit of personal income tax file or deportation in cases where national security and/or criminal enforcement is not an issue).</p>	<input checked="" type="checkbox"/> 3
<p>Criminal investigation and enforcement / National Security</p> <p>Personal information is used for investigations and enforcement in a criminal context (i.e. decisions may lead to criminal charges/sanctions or deportation for reasons of national security or criminal enforcement).</p>	<input checked="" type="checkbox"/> 4
<p>Details:</p> <p>Some personal information collected through the <i>FOTM</i> demonstration may be used in support of identifying persons who have been previously determined to be inadmissible to Canada because of known non-compliance with the <i>IRPA</i>. Therefore, this would be enforcement in a compliance and regulatory context. However, once a match occurs, CBSA secondary BSOs must independently validate the <i>FOTM</i> match with existing CBSA information systems.</p> <p>Facial photographs may be disclosed to CBSA's Inland Enforcement Division (IED), but only in the rare chance that an identified match of the <i>FOTM</i> demonstration is identified but not intercepted before leaving the terminal. In those cases, IED will utilize the <i>FOTM</i> match as a tip requiring identity validation utilizing existing systems and procedures. <i>FOTM</i> photographic and video recordings may be used as evidence to support deportation; however, it is highly unlikely. Any validation made by secondary BSOs will be used in the deportation proceedings as will video from existing Terminal 3 cameras.</p> <p>It is noted that if any PDD individuals are identified during the short-term project, they are immediately deported without any judicial review. As the PDD is comprised of individuals who have been deported and have re-entered Canada at least one time after the initial deportation, judicial</p>	

review is not available to them. Therefore, if any individual on the Previously Deported List is identified by the project, there is no sharing of the project data to the Department of Justice (DOJ), Public Prosecution Service of Canada (PPSC), Immigration and Refugee Board (IRB), or any other organization.

Privacy risk:

Some personal information collected through the *FOTM* demonstration may be disclosed to internal stakeholders, such as CBSA IED, for the purposes of compliance/regulatory enforcement.

Mitigation:

FOTM data will rarely, if ever, be used to support a deportation proceeding, but it is possible. As stated above, if a secondary BSO, using existing systems and procedures, identifies an individual as being on the Previously Deported list (maintained outside the *FOTM* FR system), then non-*FOTM* data, including video from existing Terminal 3 cameras will be used to support the deportation proceeding.

Facial photographs owned by the CBSA may be disclosed to Face4 Systems, the technology integrator, so that they can analyze and improve the effectiveness of the technology.

Facial photographs will only be disclosed in accordance with all relevant legislation and policy.

B. Type of Personal Information Involved and Context

Level of Risk

Only personal information, with no contextual sensitivities, collected directly from the individual or provided with the consent of the individual for disclosure under an authorized program.

☐ 1

Personal information, with no contextual sensitivities after the time of collection, provided by the individual with consent to also use personal information held by another source.

☐ 2

Social Insurance Number, medical, financial or other sensitive personal information and/or the context surrounding the personal information is sensitive. Personal information of minors or incompetent individuals or involving a representative acting on behalf of the individual.

☒ 3

Sensitive personal information, including detailed profiles, allegations or suspicions, bodily samples and/or the context surrounding the personal information is particularly sensitive.

☐ 4

Details:

FOTM photographs contain only the physical appearance of the traveller's face, with no context other than a date/time stamp. Scene-video clips will contain the traveller's overall appearance, behaviour, and, possibly, carry-on items. The PDD will contain additional information such as name, date of birth, and any safety warnings (where the person is considered a potential danger or threat to CBSA employees). The project cameras will photograph all persons entering the CBSA-controlled areas of Pearson International Airport's Terminal 3; this could include minors and incompetent individuals. Facial photographs will be collected directly from the individuals. PDD information will come from the CBSA's existing Previously Deported Persons database. Such use is consistent with the purposes for

which the information was collected in the first instance.

Privacy risk:

The CBSA collects a wide variety of personal information through its activities. *FOTM* photographs, scene video, and the PDD will contain minimal information, such as facial image, name, date of birth, and security warnings. The presence of an individual's information on the PDD will indicate that the individual is inadmissible to Canada. The presence of an individual's photograph in the set of facial photographs could lead to the inference that the individual attempted to enter Canada at a certain date and time.

Mitigation:

The CBSA will collect only the personal information necessary to effectively carry out its mandate.

In accordance with the CBSA's audio-visual policy, information collected for the *FOTM* demonstration will be considered to be Protected B. All photographs, videos, and PDD information, regardless of storage medium, will be stored either in a locked cabinet (or container or a safe) or in a secure room designed in accordance with specifications approved by the Infrastructure and Information Security Division of CBSA.

All retention and disposal of facial photographs, video, and PDD information will be carried out in accordance with the relevant provisions of the *AV Policy*.

The retention period for facial photographs having no enduring value to the Agency will be the duration of the project (which is scheduled to end at the end of the lab phase). All information is required until the end of the project so that the technology's performance can be evaluated. For all photographs requiring further action on the part of the CBSA, the CBSA has established a minimum two-year retention period in accordance with paragraph 4(1)(a) of the *Privacy Regulations*. In addition, if an ATIP request or formal complaint is received within 30 days of the creation of a facial photograph, that photograph will also become subject to the minimum two-year retention period.

In the context of the proposed demonstration of *FOTM* technology, it is essential to take facial images captured at Terminal 3 and replay them in the lab to further test and investigate the performance of the technology. Thus, it is necessary to retain the facial images captured during the demonstration for the duration of the project.

The AV Policy requires that:

- All disclosure of audio-video or photographic records must be made in accordance with the provisions of the *Customs Act*, the *Access to Information Act*, the *Privacy Act* and/or CBSA disclosure policy.
- When an audio-video or photographic record is disclosed in response to an ATIP request from an individual whose information is contained in the record, the identity and other personal information of other individuals in the audio-video or photographic record who are not implicated in the request will be protected. If the personal information of a third party cannot be protected, and consent has not been provided for its disclosure, the audio-video or photographic record will not be disclosed.

PROTECTED B

Faces on the Move: Multi-camera Screening

PIA

C. Program or Activity Partners and Private Sector Involvement

Level of Risk

- | | |
|--|---------------------------------------|
| Within the institution (amongst one or more programs within the same institution) | <input type="checkbox"/> 1 |
| With other federal institutions | <input type="checkbox"/> 2 |
| With other or a combination of federal/ provincial and/or municipal government(s) | <input type="checkbox"/> 3 |
| Private sector organizations or international organizations or foreign governments | <input checked="" type="checkbox"/> 4 |

Details:

Facial photographs, scene video, and PDD information will be disclosed to integration firm Face4 Systems so that they can "re-play" the photo stream in a lab setting and fine-tune the performance of the technology. The facial photographs, scene video, and PDD information may also be accessible to the telecommunications provider that will operate the wireless link that is part of the demonstration architecture.

Performance metrics will be shared with staff of ÉTS who will provide analytical assistance regarding project evaluation. ÉTS staff will not have access to any information defined as "personal information" by the *Privacy Act*.

Privacy risk:

Facial photographs, scene video, or PDD information will be disclosed to Face4 Systems. Facial photographs, scene video, or PDD information may be accessible by the telecommunications provider.

Mitigation:

The AV Policy states:

- All disclosure of audio-video or photographic records must be made in accordance with the provisions of the *Customs Act*, the *Access to Information Act*, the *Privacy Act* and/or CBSA disclosure policy.

In addition, the *Directives on the Overt Use of Audio-Video Monitoring and Recording Technology* state that:

- Any access to or disclosure of audio-video or photographic recordings must be noted in an audio-video monitoring log. The log entry must include the date and time when the data was accessed, which segment of the data was viewed, by whom and for what reason. Persons who access recordings must identify themselves by name and badge number if applicable. When a recording is disclosed, the authority for that disclosure must also be noted in the log.
- When audio-video or photographic recordings are copied or extracted in order to be disclosed within the CBSA or to other organizations, the CD, DVD or storage device must be stored in locked storage according to the security classification of the information contained in the audio-video recording. Facial photographs and related information are to be categorized as Protected B.
- Audio-video or photographic recordings, including records to be disclosed to organizations, may only be disclosed as authorized by the *Privacy Act*, s. 8, *Customs Act*, s. 107, and CBSA disclosure policy.
- Only the segment of the audio-video recording or the photograph or PDD information related to the request will be provided. Any unrelated data will be blacked-out, blurred, or obscured by a technique certified as tamper-proof by a credible certification body.

PROTECTED B

Faces on the Move: Multi-camera Screening

PIA

D. Duration of the Program or Activity

Level of risk

One time program or activity

☐ 1

Typically involves offering a one-time support measure in the form of a grant payment as a social support mechanism.

Short-term program

☒ 2

A program or an activity that supports a short-term goal with an established "sunset" date.

Long-term program

☐ 3

Existing program that has been modified or is established with no clear "sunset".

Details:

The CBSA will deploy the *FOTM* technology in the short-term context of a technology demonstration. The technology will be installed in Terminal 3 of Pearson International Airport for a period of six months and then removed. The technology will be re-installed in a lab setting in Ottawa to allow researchers to further investigate and study its performance by replaying images retained from the live demonstration.

Privacy Risk:

The CBSA will collect personal information for *FOTM* for a limited time. Analysis of the results of the demonstration will contribute to senior management decisions on further testing and evaluation of FR technology.

Mitigation:

The CBSA will only retain personal information for the minimum amount of time necessary to ensure it is of no enduring value to the Agency, with all records scheduled to be destroyed at the end of the project.

In order to balance the privacy rights of individuals with the needs of the CBSA to ensure the safety and security of Canada, it has been established that the minimum retention period for facial photographs and scene video attached to matches will be the duration of the project. Scene video having no enduring value to the Agency (i.e., scene video that is not linked to any matched travellers) will be retained for 30 days, in accordance with the *AV Policy*. For all facial photographs, scene video, or PDD information requiring further action on the part of the CBSA, the CBSA has established a minimum two-year retention period in accordance with paragraph 4(1)(a) of the *Privacy Regulations*. In addition, if an ATIP request or formal complaint is received within 30 days of the creation of a recording, that recording will also become subject to the minimum two-year retention period.

E. Program Population

Level of Risk

The program affects certain employees for internal administrative purposes.

☐ 1

The program affects all employees for internal administrative purposes.

☐ 2

The program affects certain individuals for external administrative purposes.

☒ 3

The program affects all individuals for external administrative purposes.

☐ 4

Details:

Some information collected will be disclosed within the CBSA for the purpose of determining a traveller's admissibility to Canada.

Privacy Risk:

Facial photographs of travellers, scene videos, or PDD information used to refer an individual who matches to the PDD may be disclosed within the CBSA.

Mitigation:

The CBSA will ensure that any disclosure of facial photographs, scene video, or PDD information is made in accordance with the relevant policies and legislation. After the initial six-month demonstration at Terminal 3 of Pearson International Airport, the system will be re-located to the CBSA's SED lab (Ottawa) for up to six more months of further tests. This includes re-running the photographs taken in Terminal 3 against the PDD and modifying the matching parameters in tests to improve system performance.

F. Technology and Privacy

6.1 Does the new or modified program or activity involve the implementation of a new electronic system, software or application program including collaborative software (or groupware) that is implemented to support the program or activity in terms of the creation, collection or handling of personal information? ☒ YES ☐ NO

6.2 Does the new or modified program or activity require any modifications to IT legacy systems and / or services? ☐ YES ☒ NO

6.3 Does the new or modified program or activity involve the implementation of one or more of the following technologies:

6.3.1 Enhanced identification methods:

This includes biometric technology (i.e. facial recognition, gait analysis, iris scan, fingerprint analysis, voice print, radio frequency identification (RFID), etc...) as well as easy pass technology, new identification cards including magnetic stripe cards, "smart cards" (i.e. identification cards that are embedded with either an antenna or a contact pad that is connected to a microprocessor and a memory chip or only a memory chip with non-programmable logic).

☒ YES
☐ NO

Please specify:

The CBSA will use *FOTM* in approaches to the arrivals hall, approaches to PIL booths, during PIL interviews, and approaches to immigration point to identify persons of interest to the CBSA through matching facial images with PDD images.

6.3.2 Use of Surveillance:

This includes surveillance technologies such as audio/video recording devices, thermal imaging, recognition devices, RFID, surreptitious surveillance / interception, computer aided monitoring including audit trails, satellite surveillance etc.

☒ YES
☐ NO

Please specify:

FOTM will use cameras to overtly photograph travellers' faces and to record scene video of the travellers' overall appearances (e.g., clothing, luggage, companions).

6.3.3 Use of automated personal information analysis, personal information matching and knowledge discovery techniques:

☒ YES
☐ NO

For the purposes of the Directive on PIA, government institutions are to identify those activities that involve the use of automated technology to analyze, create, compare, cull, identify or extract personal information elements. Such activities would include personal information matching, record linkage, personal information mining, personal information comparison, knowledge discovery, information filtering or analysis. Such activities involve some form of artificial intelligence and/or machine learning to uncover knowledge (intelligence), trends/patterns or to predict behaviour.

Please specify:

The CBSA will use *FOTM* to compare images of arriving travellers' faces with facial photographs of persons of interest on a PDD. The technology will identify potential matches and notify CBSA officers, who will manually review and adjudicate the potential matches. Real-time matches that are verified by human review will be forwarded to roving CBSA officers for further action.

A **YES** response to any of the above indicates the potential for privacy concerns and risks that will need to be considered and if necessary mitigated.

6.1 Implementation of new cameras, FR servers, and wireless communications.

Privacy Risk:

The CBSA will implement cameras that have the capability to take facial photographs of any and all individuals found in CBSA-controlled and -monitored areas accessible to the travelling public. Facial images of immediately verified persons of interest will be transmitted wirelessly within the CBSA-controlled and CBSA-monitored areas to notify roving CBSA officers of the presence of a person of interest. The CBSA will also implement video cameras to take scene video of the same areas. The system will attach a short video clip (approximately 5 seconds) to each match record to provide context of the traveller within the airport.

Mitigation:

Facial photographs and scene video taken by the on-site cameras and information contained in the PDD will be accessible only to properly authorized and trained CBSA personnel. This information will be used only to identify persons of interest who have already been determined to be inadmissible to Canada and to perform post-demonstration tests and analysis on the FR technology in a CBSA lab setting. The facial photographs and scene video taken on-site will have no identifying information associated with them other than a date/time stamp. The PDD will contain only photographs, names, birthdates, and safety warnings. Information about potential matches will be retained for the duration of the project to generate metrics about the performance of the technology.

Live-captured facial photographs and scene video for matched travellers will be retained for the duration of the project. Unused scene video (i.e., video that is not linked to any matched travellers) will be retained for 30 days from the time of creation. PDD information will be retained for the duration of the project.

6.3.1 Enhanced identification methods

Privacy Risk:

The CBSA will use *FOTM* to compare photographs of travellers' faces with images stored in a PDD to identify persons who have already been determined to be inadmissible to Canada. There is a risk that an individual will be incorrectly matched with a PDD entry and be selected for secondary examination as a result of the false match. There is a further risk that a falsely matched traveller selected for secondary examination could learn the identity of the person of interest on the PDD against whom he or she was incorrectly matched.

Mitigation:

An important objective of the *FOTM* demonstration is to assess the readiness of the FR technology, including its ability to minimize false matches. Procedures will be developed to quickly ascertain the identity of travellers selected on the basis of *FOTM* for secondary examination using existing CBSA systems. Persons who have been deemed to be incorrectly matched with a PDD entry will be released as quickly as possible, assuming no other questions arise about the traveller's identity and admissibility (it is possible that a traveller matched incorrectly and selected for secondary examination is still found to be inadmissible for other reasons).

Furthermore, the CBSA will develop procedures to ensure that, when questioning a traveller who has been selected for secondary examination on the basis of *FOTM*, the traveller will not be told the name of the person on the PDD against whom the traveller has been matched. The traveller will not be shown the photograph of the person on the PDD. This will ensure that falsely matched travellers are not inadvertently given information about persons of interest.

6.3.2 Use of surveillance

Privacy Risk:

The CBSA will use cameras to overtly record travellers' facial images and physical appearance. Although there is a reduced expectation of privacy at an airport, travellers may perceive a risk that unauthorized personnel could access the images taken by *FOTM*.

Mitigation:

The CBSA will ensure that any disclosure of facial photographs, scene video, or PDD information is made in accordance with the relevant policies and legislation. In addition, the CBSA will take steps to ensure that recordings are not disclosed by third parties without the consent of the CBSA. After the initial six-month demonstration at Terminal 3 of Pearson International Airport, the system will be re-located to the CBSA's SED lab (Ottawa) for six more months of further tests. This includes re-running the photographs taken in Terminal 3 against the PDD and modifying the matching parameters in tests to improve system performance.

The CBSA's AV Policy states:

- All disclosure of audio-video or photographic records must be made in accordance with the provisions of the *Customs Act*, the *Access to Information Act*, the *Privacy Act* and/or CBSA disclosure policy.

In addition, the CBSA's *Directives on the Overt Use of Audio-Video Monitoring and Recording Technology* state that:

- Any access to or disclosure of audio-video or photographic recordings must be noted in an audio-video monitoring log. The log entry must include the date and time when the data was accessed, which segment of the data was viewed, by whom and for what reason. Persons who access

recordings must identify themselves by name and badge number if applicable. When a recording is disclosed, the authority for that disclosure must also be noted in the log.

- When audio-video or photographic recordings are copied or extracted in order to be disclosed within the CBSA or to other organizations, the CD, DVD or storage device must be stored in locked storage according to the security classification of the information contained in the audio-video recording. Facial photographs and related information are to be categorized as Protected B.
- Audio-video or photographic recordings, including records to be disclosed to organizations, may only be disclosed as authorized by the *Privacy Act*, s. 8, *Customs Act*, s. 107, and CBSA disclosure policy.
- Only the segment of the audio-video recording or the photograph or PDD information related to the request will be provided. Any unrelated data will be blacked-out, blurred, or obscured by a technique certified as tamper-proof by a credible certification body.

6.3.3 Use of automated personal information analysis, personal information matching and knowledge discovery techniques

Privacy Risk:

The CBSA will use FR to compare photographs of travellers' faces with images stored in a PDD to identify persons who may be inadmissible to Canada. There is a risk that an individual will be incorrectly matched with a PDD entry and be selected for secondary examination as a result of the false match. There is a further risk that a falsely matched traveller selected for secondary examination could learn the identity of the person of interest on the PDD against whom he or she was incorrectly matched.

Mitigation:

An important objective of the *FOTM* demonstration is to assess the readiness of the FR technology, including its ability to minimize false matches. Procedures will be developed to quickly ascertain the identity of travellers selected for secondary examination on the basis of *FOTM* using existing CBSA systems. Persons who have been deemed to be incorrectly matched with a PDD entry will be released as quickly as possible, assuming no other questions arise about the traveller's identity and admissibility (it is possible that a traveller matched incorrectly and selected for secondary screening is still found to be inadmissible for other reasons).

Furthermore, the CBSA will develop procedures to ensure that, when questioning a traveller who has been selected for secondary examination on the basis of *FOTM*, the traveller will not be told the name of the person on the PDD against whom the traveller has been matched. The traveller will not be shown the photograph of the person on the PDD. This will ensure that falsely matched travellers are not inadvertently given information about persons of interest.

G. Personal Information Transmission

Level of Risk

The personal information is used within a closed system.

☐ 1

No connections to Internet, Intranet or any other system. Circulation of hardcopy documents is controlled.

The personal information is used in system that has connections to at least one other system.

☐ 2

PROTECTED B

Faces on the Move: Multi-camera Screening

PIA

The personal information is transferred to a portable device or is printed.

☐ 3

USB key, diskette, laptop computer, any transfer of the personal information to a different medium.

The personal information is transmitted using wireless technologies.

☒ 4

Details:

Match alerts will be sent wirelessly from the match adjudication officer in the CBSA surveillance centre to roving CBSA officers in the CBSA-controlled areas of Terminal 3 of Pearson International Airport. Match alerts will contain a photo, a short video clip, and biographical information about the person of interest (name, date of birth, safety warning (if applicable)). The wireless technology used is most likely to be a commercially-operated cellular communications link (Wi-Fi service in Terminal 3 is inadequate for the demonstration).

Privacy Risk:

The personal information being transmitted on a wireless network may be compromised. A wireless network is necessary for match alerts because the receiving CBSA officer is patrolling the airport and cannot be reached via a wired connection.

Mitigation:

The CBSA will ensure that all wireless transmission of data is secure using appropriate encryption technologies. Any transmission of recordings over wireless networks must be done in accordance with the CBSA's *Policy on the Use of Wireless Technologies*. Wireless transmission of data not in compliance with these protocols must cease immediately and the wireless transmission can only resume when authorized by local IT and an official of the Physical Security Section of the Security and Professional Standards Directorate. A Security Assessment of *FOTM*, including wireless alert transmission, is underway and will be forwarded when it is complete.

H. Risk Impact to the Institution

Level of Risk

Managerial harm.

☐ 1

Processes must be reviewed, tools must be changed, change in provider / partner.

Organizational harm.

☒ 2

Changes to the organizational structure, changes to the organizations decision-making structure, changes to the distribution of responsibilities and accountabilities, changes to the program activity architecture, departure of employees, reallocation of HR resources.

Financial harm.

☐ 3

Lawsuit, additional moneys required reallocation of financial resources.

Reputation harm, embarrassment, loss of credibility.

☐ 4

Decreased confidence by the public, elected officials under the spotlight, institution strategic outcome compromised, government priority compromised, impact on the Government of Canada Outcome areas.

Details:

The CBSA has implemented appropriate controls to safeguard the privacy of all persons affected by

FOTM. If the photographs, scene videos, or PDD information are compromised or otherwise released without authority to do so, the CBSA may have to review its programs and organizational structures to determine whether deficiencies in those programs and structures contributed to a privacy breach. Changes to the admissibility determination program and associated organizational structures may be required to prevent similar future breaches.

Privacy Risk:

Should records be inadvertently or inappropriately released, this may reflect on deficiencies in the CBSA's organizational structures and its admissibility determination program in terms of their ability to properly implement the required privacy controls.

Mitigation:

The CBSA will take steps as recommended in the accompanying Security Assessment Summary to ensure that the organization in general and the *FOTM* project in particular (as deployed at Terminal 3 of Pearson International Airport) are briefed and trained on the proper application of required privacy controls. Only those employees who require access to records as part of their official duties and who have a need to view them will be permitted to access them. Such permission will be granted in writing and all access to records will be monitored by way of access logs.

I. Risk Impact to the Individual or Employee

Level of Risk

- | | |
|---------------------------------|---------------------------------------|
| Inconvenience. | <input type="checkbox"/> 1 |
| Reputation harm, embarrassment. | <input checked="" type="checkbox"/> 2 |
| Financial harm. | <input type="checkbox"/> 3 |
| Physical harm. | <input type="checkbox"/> 4 |

Details:

The inadvertent disclosure of such information without authorization or to an improper party may lead to harm to reputation and/or embarrassment. For example, details surrounding an individual's travel including date, time, and location of arrival may be contained in recordings.

Privacy Risk:

Should recordings be inadvertently or inappropriately released, there is a risk that individuals whose information is contained in those recordings could suffer reputation harm or embarrassment given the sensitivities surrounding the information that is collected and the potential impact the release could have on those individuals.

Mitigation:

As above, the CBSA will take steps to ensure that disclosure of recordings is only made in accordance with the relevant legislation as indicated above. Only those employees with a minimum SECRET security clearance who require access to recordings as part of their official duties and who have a need to view them will be permitted to access them. Such permission will be granted in writing and all access to recordings will be monitored by way of access logs.

For Internal Use Only – Distribution Limited to Project Personnel

Faces on the Move: Multi-camera Screening

PIA

SECTION 5 – ANALYSIS OF PERSONAL INFORMATION ELEMENTS

Personal Information Elements and Sub-elements

Note: Identification of sub-elements is necessary where sensitive personal information is being collected or where the type of program or activity presents a potential privacy risk at level 2-3-4 in “Section 3 - Risk Identification and Categorization” of the PIA.

Category Of Personal Information	Personal Information Element	Personal Information Sub-Element	Format	Purpose / Necessity of Element
Gender, physical attributes	Physical image of traveller when photo or scene video is captured.	<ul style="list-style-type: none"> includes a person's race, ethnic origin, or colour can include information related to a person's employment (e.g., from employment-related headwear or clothing) can include information related to a person's religious affiliation (e.g., from clothing or accessories) 	Visual Image Recording, stored as digital files	<p>To identify persons known to be inadmissible.</p> <p>To assist in making admissibility decisions regarding the entry of persons to Canada.</p> <p>To ensure the integrity of the immigration program.</p>
Gender, physical attributes, name, date of birth, safety warnings	Physical image of person and associated details when information is collected from existing sources for PDD.	<ul style="list-style-type: none"> includes a person's race, ethnic origin, or colour Name (and possibly known aliases) Date of birth Safety warnings (such as flight risk, risk of violence, etc.) 	Electronic database entries, including digital images	<p>To match against live-capture photos to identify persons inadmissible to Canada.</p> <p>To assist in making admissibility decisions regarding the entry of persons to Canada.</p> <p>To ensure the integrity of the immigration program.</p>

For Internal Use Only – Distribution Limited to Project Personnel

Faces on the Move: Multi-camera Screening

PIA

Biometric Information	Biometric Information	<ul style="list-style-type: none"> • FR algorithm 	Electronic database entries, including digital images	<p>To match against live-capture photos to identify persons inadmissible to Canada.</p> <p>To assist in making admissibility decisions regarding the entry of persons to Canada.</p> <p>To ensure the integrity of the immigration program.</p>
-----------------------	-----------------------	--	---	---

SECTION 6 - FLOW OF PERSONAL INFORMATION

Identify the flow of the personal information within and outside the institution's program or activity. Institutions may choose to outline the flow of personal information in the format of their choice.

FR Information Flow Model - Diagrams

The flow of personal information within the *FOTM* system is depicted using data flow diagrams (DFDs) on the following pages. There are four types of symbols used in these diagrams:

- Sharp-cornered rectangle: represents an external entity that provides information to the system or receives information from it
- Round-cornered rectangle: represents a process where information inputs are transformed into information outputs
- Open-ended rectangle: represents a repository where information is stored
- Arrow: represents a flow of information

Each shape is labelled to describe its purpose or content.

The DFDs are presented as a hierarchical model of the system. The first diagram is a high-level overview of the system, showing the system as a single process exchanging information with various external entities. The next diagram decomposes that single process into five sub-processes. The following diagrams decompose four of those sub-processes to a greater level of detail. The fifth sub-process is straightforward and requires no further decomposition.

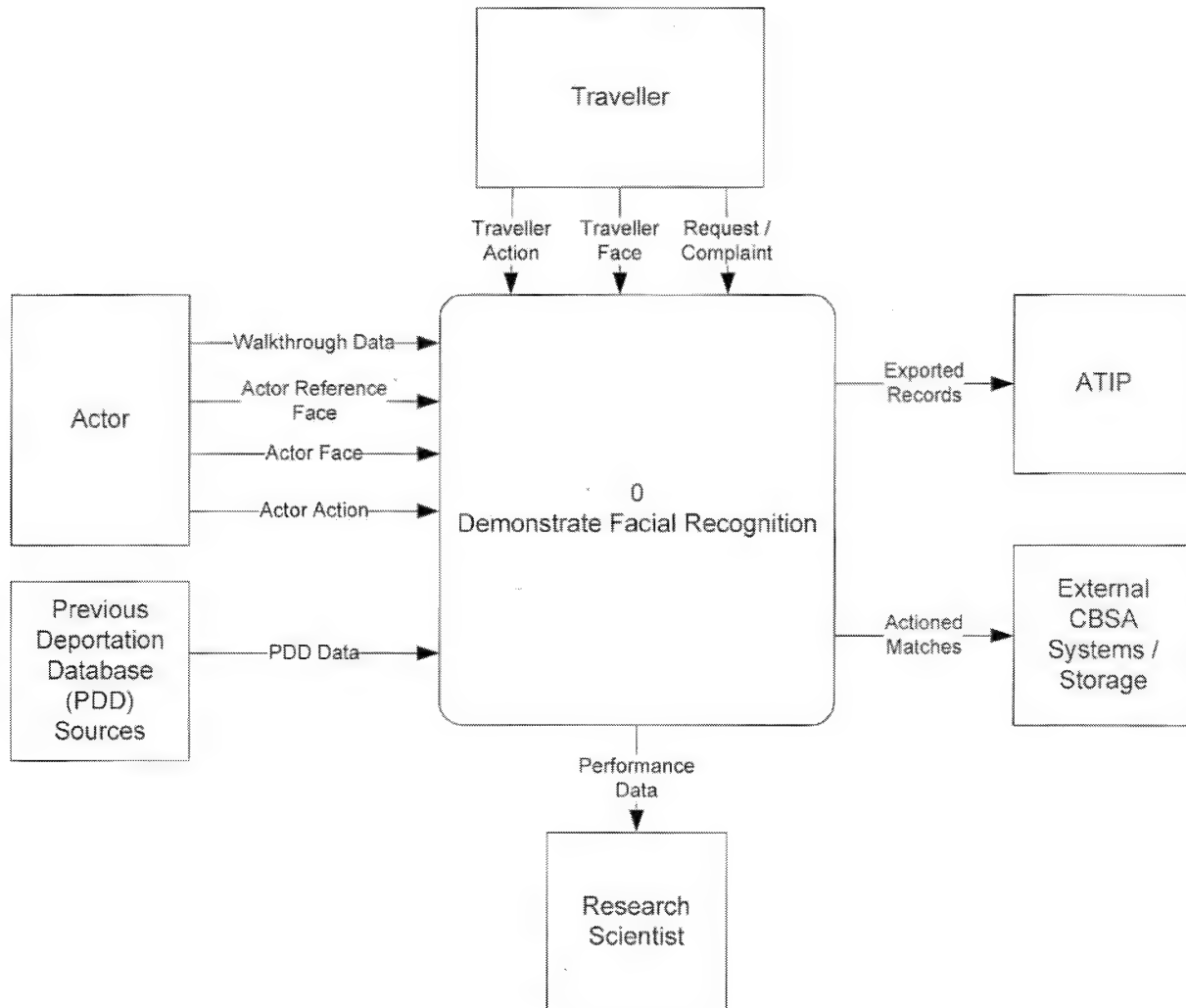


Figure 2: High-level Data Flow Diagram – Faces on the Move

The Traveller entity in

Figure 2 represents all travellers who pass through the international area of Terminal 3 of Pearson International Airport during the course of the *FOTM* demonstration. Travellers' faces and actions will be recorded as part of the main task of demonstrating FR. Travellers (or their representatives) may also file access to information requests or privacy complaints regarding the information collected from them.

The Actor entity represents CBSA employees who volunteer to participate in the *FOTM* demonstration to help researchers calibrate the FR technology. We cannot be certain that any travellers on the PDD will pass through the airport during the time of the demonstration. Actors are required to help demonstrate the readiness level of the technology by walking through the airport at known times. Actors' faces and actions will be recorded, just like those of travellers. In addition, actors will be enrolled into the PDD through a posed facial photograph (the "reference face" data flow). Finally, actors will provide information about each walkthrough (time and actor identity). The FR system will include actual photographs of the actors but with accompanying fictitious biographical data.

The PDD Sources entity represents all entities (external to *FOTM*) that provide the source data for constructing the operational PDD (i.e., the entries that do not come from actors). This is expected to include GTAR's existing database of Previously Deported Persons. All personal information will be handled in accordance with existing procedures and requirements.

The Research Scientist entity represents those individuals who will be analyzing and evaluating the performance of the FR technology, which will include individuals from the CBSA, Face4 Systems, and ÉTS; however, ÉTS will not have access to any personal information (performance metrics only).

The External CBSA Systems / Storage entity represents a CD, USB or similar device that would receive information related to travellers who have been directly affected by the *FOTM* demonstration. If the system and the primary adjudicator match a traveller to an entry on the operational PDD, CBSA will attempt to locate that traveller within the CBSA-controlled areas of Terminal 3 of Pearson International Airport and interact with him or her in accordance with existing procedures. According to current CBSA policies, the information that led to this interaction with the traveller must be kept for two years. The *FOTM* demonstration is only in operation for a short time, so information that led to action with respect to a matched traveller will be exported to other CBSA systems to be retained for the required period.

Information validated independently by the Immigration Secondary BSOs may be stored in existing CBSA systems, but not until an independent identity validation task has been completed.

The ATIP entity represents that branch of the CBSA (Access to Information and Privacy) that will extract information from the system to respond to traveller requests and complaints. The interaction between ATIP and the traveller is outside the scope of *FOTM* and is not directly represented in this model. below decomposes the high-level process into five numbered sub-processes.

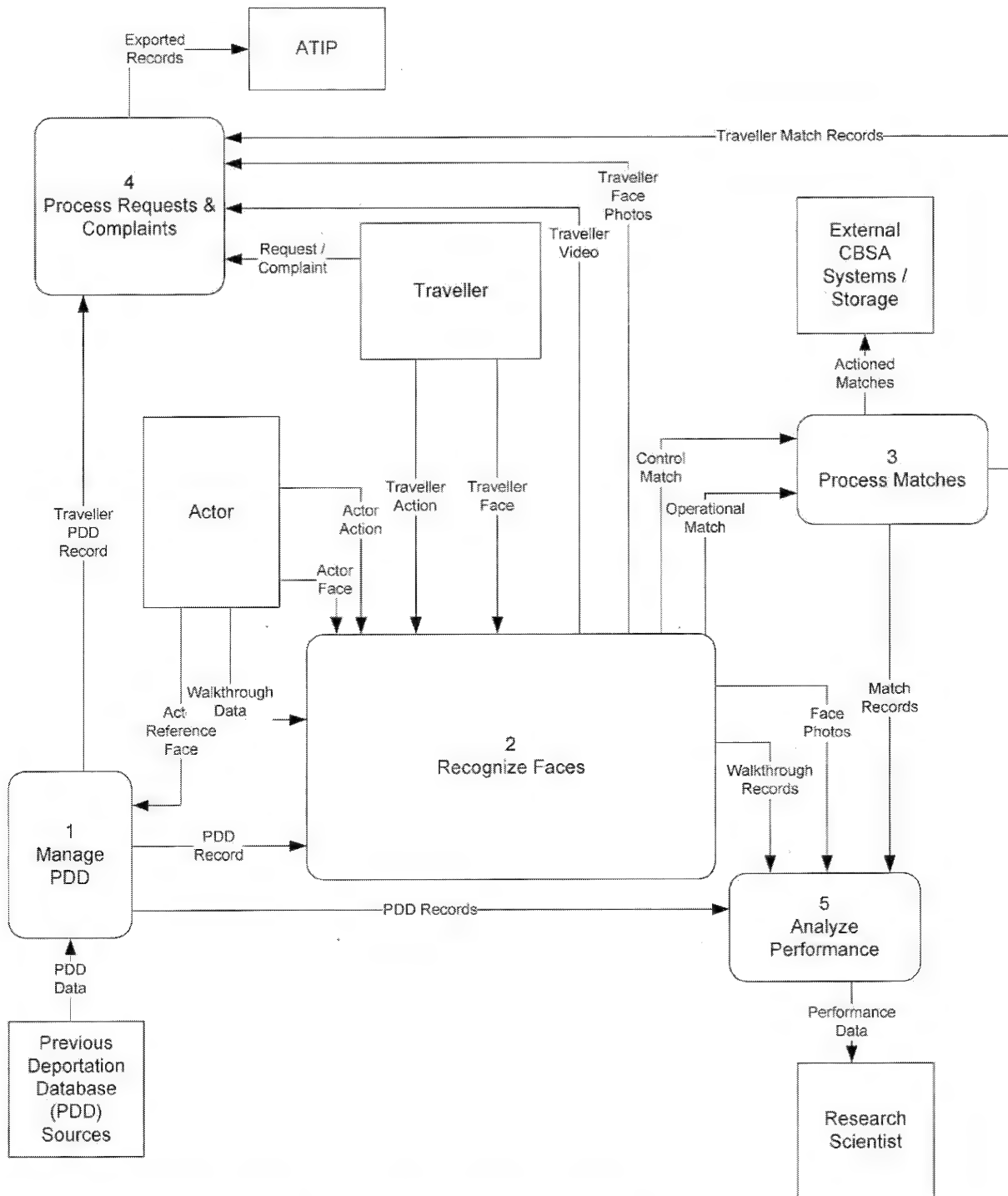


Figure 3: Data Flow Diagram – Demonstrate Facial Recognition

The five sub-processes are as follows:

1. Manage PDD – extract PDD data from external systems and actors and create PDD entries; present PDD records to other processes as needed
2. Recognize Faces – record the faces and actions of travellers and actors and identify those that match entries in the PDD; determine which matches are control (actor) matches and which are operational (traveller) matches; extract relevant video footage for operational matches
3. Process Matches – humans adjudicate each system-identified match either in real time or after the fact; act on adjudicated real-time operational matches; export match data to external systems when a matched traveller is affected
4. Process Requests & Complaints – find relevant records within the system for any traveller that submits a request or complaint about the personal information collected from him/her
5. Analyze Performance – evaluate how well the system identified actors; re-run the original photos while adjusting performance parameters to improve the detection rate while minimizing the false acceptance and false rejection rates

Figure 4 below expands the PDD process.

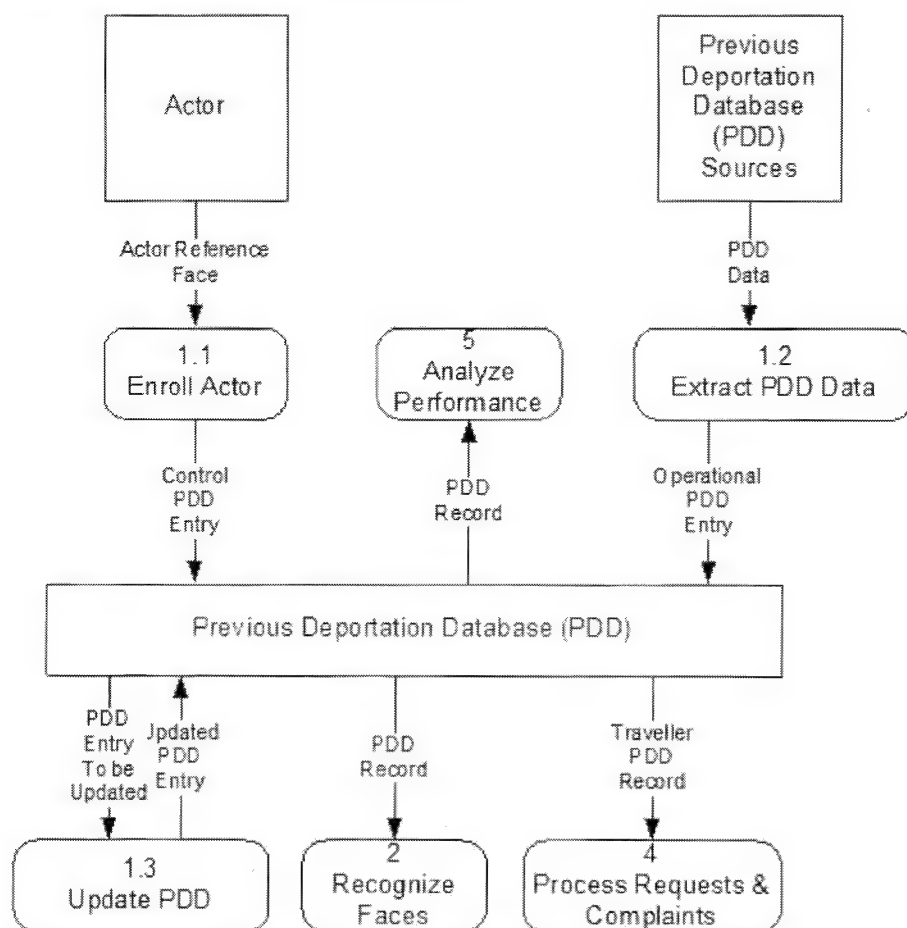


Figure 4: Data Flow Diagram - Manage Previous Deportation Database (PDD)

PDD data will be extracted from an existing CBSA regional database which stores information and photos on Previously Deported Persons (process 1.2). The size of the PDD will be limited to

approximately 5,000 records for the *FOTM* demonstration. The primary criterion for selecting records is that a person has been deported two or more times in the past three years; however, the project will not include any individual who meets this criterion if the photograph of the individual is not of sufficient quality to support the FR technology.

Each entry in the PDD will contain a photo of the person of interest (taken by CBSA before a prior deportation), the person's name, date of birth, a FOSS ID number (which links the entry to a record in the Field Operations Support System (FOSS)²), and any warnings associated with the person (such as safety warnings, threat warnings, health warnings, etc.).

PDD data will be extracted to allow the CBSA to carry out its mandate to detect and identify persons who have a record of failing to comply with the *Immigration and Refugee Protection Act*.

Control PDD data, including photos, will be collected directly from actors (CBSA employees who volunteer; process 1.1). The control PDD will contain information about known individuals who will, over the course of the demonstration, walk past the cameras to test the performance of the FR technology. These control PDD entries will be similar in structure to operational PDD entries, but with an extra note that they are control entries. The control photos will be of real individuals, but the biographical information will be test data.

All PDD entries (operational and control) will be securely stored as per CBSA policies on the storage of protected information (refer to Appendix: Comptrollership Manual - Security Volume – Chapter 6: Storage of Sensitive Information and Assets). The data store for PDD entries will be dedicated to the *FOTM* demonstration. This data store will not be connected to any other CBSA systems or programs. It is expected that the PDD entries will be in the form of relational database records, including the photo images.

The system will include a capability to allow PDD entries to be manually updated or deleted (process 1.3). New PDD entries may be added during the six months of the demonstration on an *ad hoc* basis. These *ad hoc* additions will use the same procedures as the initial entries and would include any new Previously Deported Person who meets the initial selection criteria or new actors

Figure 5 on the next page expands the Recognize Faces process.

² FOSS is in the process of being replaced by a new system called the Global Case Management System (GCMS), but "FOSS ID" is still the term used to refer to specific files or cases.

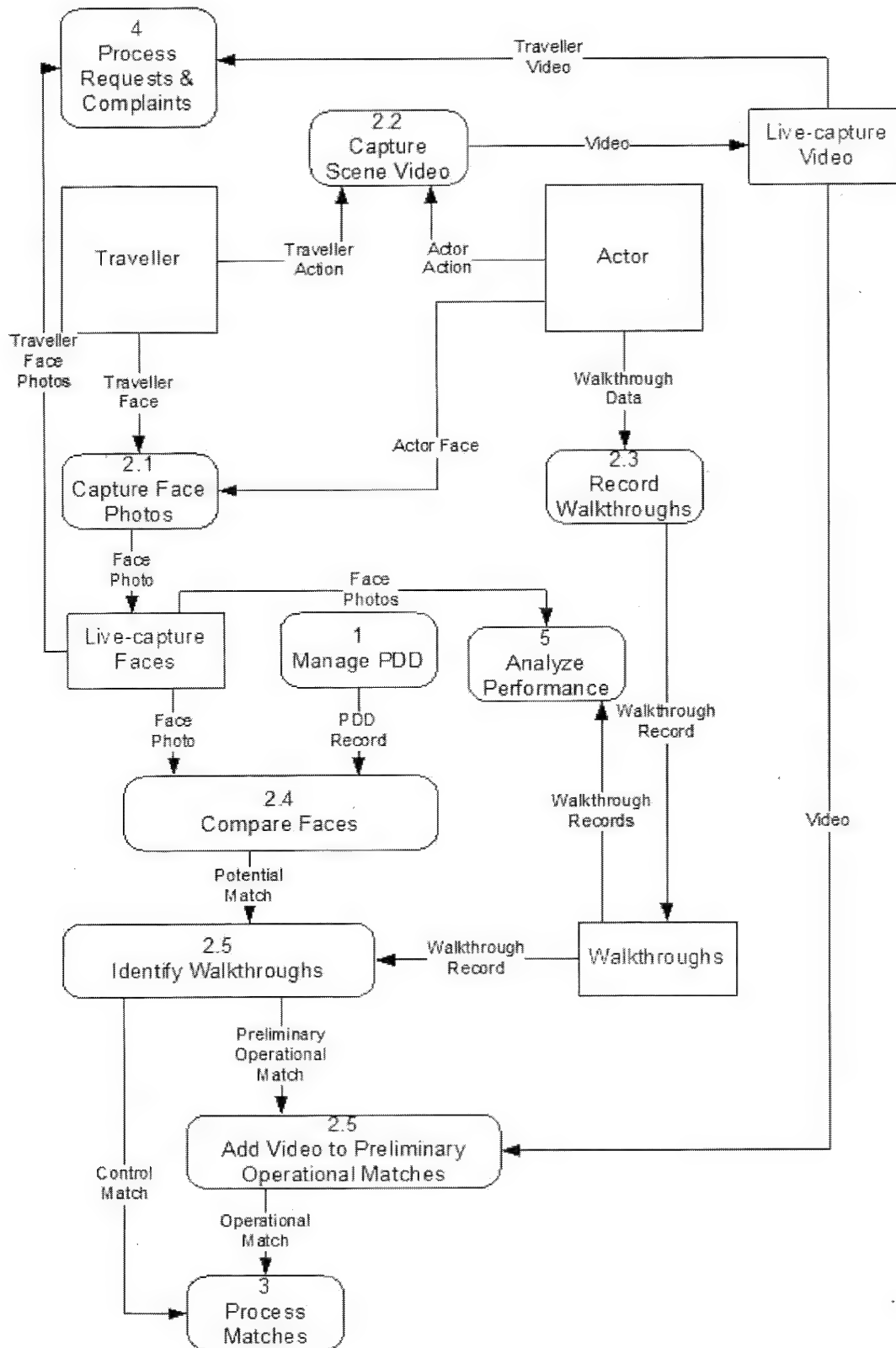


Figure 5: Data Flow Diagram - Recognize Faces

Travellers and actors will walk through the CBSA-controlled areas of Terminal 3, Pearson International Airport, such as the arrivals hall, the approaches to the PIL booths, the PIL booths themselves, and the approach to the immigration point. Actors will inform the system when they have performed a walkthrough (process 2.3). This will likely be by swiping an identification card at a special-purpose card reader. The date and time of the walkthrough and an identifier of the actor will be recorded as walkthrough data. This information is required to analyze performance and accuracy of the FR technology. This information will be stored as per CBSA policies on the storage of protected information when they are not in use. (Refer to Appendix: Comptrollership Manual – Security Volume – Chapter 6: Storage of Sensitive Information and Assets).

Dedicated project-cameras mounted at selected locations in the CBSA-controlled area of Terminal 3 at Pearson International Airport will record the faces of people walking through those areas (process 2.1). Dedicated project video cameras referred to as *scene cameras* will also record video of the travellers and actors (process 2.2). All facial photographs and scene video recordings will be securely stored as per CBSA policies on the storage of protected information when they are not in use. (Refer to Appendix: Comptrollership Manual – Security Volume – Chapter 6: Storage of Sensitive Information and Assets.) Photographs and video will be in the form of electronic media files.

Access to and control of any photography equipment is limited to qualified operators who are authorized to do so by the manager responsible for Terminal 3 of Pearson International Airport. Authorization is provided in writing and specifies the purposes for which access and or control is given.

As facial photographs of arriving passengers and of actors are captured, they are compared to the entries in the PDD (process 2.4).

If the FR system identifies a potential match between a live-captured photo and a PDD entry, the FR system will compare the match with the walkthrough data to determine whether the match is a test subject from the control group of actors (walkthrough; process 2.5). All potential matches that are not walkthroughs will be deemed operational. The FR system will attach to each preliminary operational match a video clip taken at the same approximate time and location as the matched face photo (process 2.5). This is to provide additional context for the match, such as the traveller's clothing, location, and companions.

All facial photographs will be retained until the end of the *FOTM* project. This is so that the stream of face photos can be re-run in a lab setting to assess and analyze the performance of the technology. All facial photographs will be securely stored as per CBSA policies on the storage of protected information when they are not in use. (Refer to Appendix: Comptrollership Manual – Security Volume – Chapter 6: Storage of Sensitive Information and Assets.) Unused scene video recordings will be deleted 30 days after creation, in accordance with the CBSA's current policies for video recordings. Video clips that end up being used to support administrative action against a traveller will be retained for two years from the date of last administrative use, in accordance with the CBSA's current policies for video recordings. (Refer to the *Policy on the Overt Use of Audio-Video Monitoring and Recording Technology*.)

Figure 6 below expands the Process Matches process.

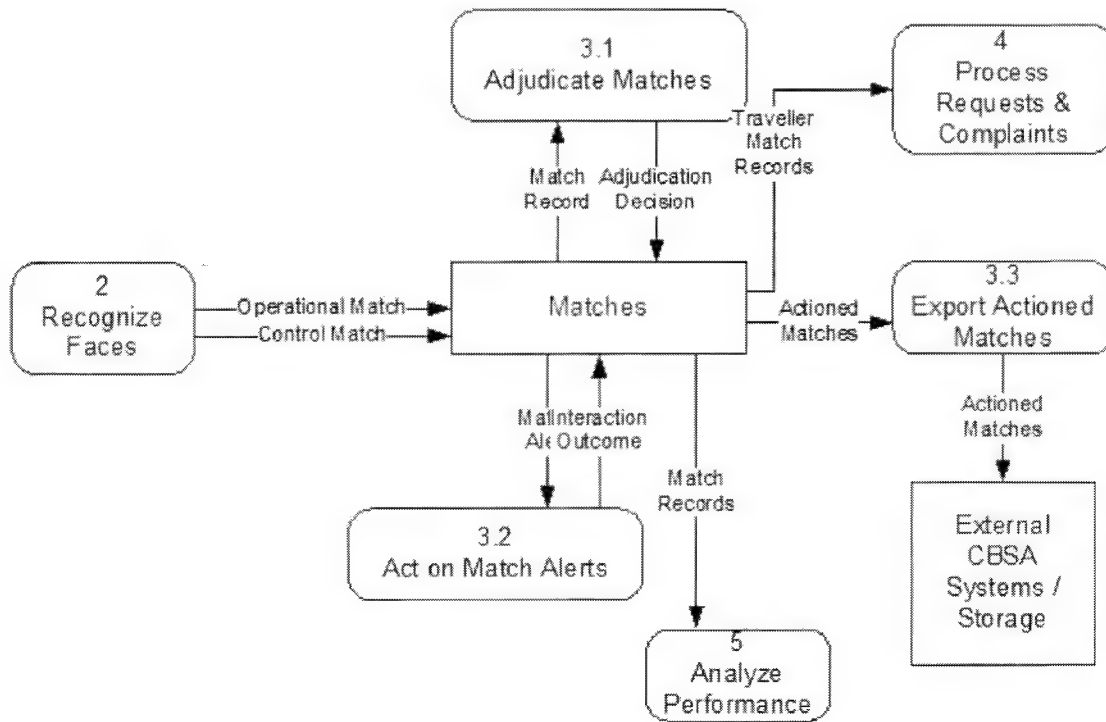


Figure 6: Data Flow Diagram - Process Matches

All matches, operational and control, will be stored in the *FOTM* system and displayed on a monitor in the Surveillance Centre. High-probability matches will be displayed immediately. Low-probability matches will be reviewed in bulk at a later time. A CBSA adjudicator (or, in the case of a low-probability match, a project scientist or technician) will review each potential match on the monitor and decide whether the match is valid (process 3.1).

The adjudicator records the adjudication decision (true or false match) in the match record in dedicated application available on a dedicated workstation; and stored on the FR server. The match record will link a live-capture image with a PDD entry. The FR system will indicate whether a match is control or operational and will link a related video clip to each operational match. The match record will also contain the adjudicator's decision to accept or reject the match.

If the match is accepted by the adjudicator and is real-time and operational (i.e., a traveller, not an actor), the FR system will send a notification over a wireless communication channel to one or more handheld devices carried by roving CBSA officers in the terminal. The adjudicator will also radio a superintendent to advise the superintendent that a match has been found and to describe verbally the physical appearance of the person, based on the scene video recording. The roving officer will use a project-specific application on the handheld device to access the match record. This allows the roving

officer to view photos, video, and information about the matched individual. The roving officer uses this information to search for and intercept the matched individual (process 3.2). If the match is rejected by the adjudicator or is a control match (i.e., an actor, not a traveller), the system takes no further action.

If the roving CBSA officer finds the matched individual, the officer will interact with the individual following standard CBSA protocols and procedures.

The CBSA officer will use the application on the handheld device to update the match record with the outcome of the officer's interaction with the matched individual or with the officer's failure to locate the matched individual. Outcomes may include: released, detained, referred to secondary, failed to intercept.

When an operational match results in action being taken with respect to a traveller, such as a referral to secondary examination, the match record, including all PDD information, live-capture photos, and scene video, will be exported to secondary storage (CD, USB or similar) in accordance with CBSA policies which require that any interaction with a traveller (i.e. referring the individual for secondary examination based on the FR solution) must be kept for two years. The storage device will be kept on the individual's file, so that a permanent record of the information that led to the action can be preserved; however, evidence supporting deportation will be limited to the identity validation efforts of the secondary immigration BSO. If deportation is the result of the secondary examination, then non-FOTM data, including video from existing Terminal 3 cameras, will be used to support the deportation proceeding. Only in rare and extraordinary cases does CBSA envision FOTM data being a supporting piece of information in a deportation proceeding.

Figure 7 below expands the Process Requests & Complaints process.

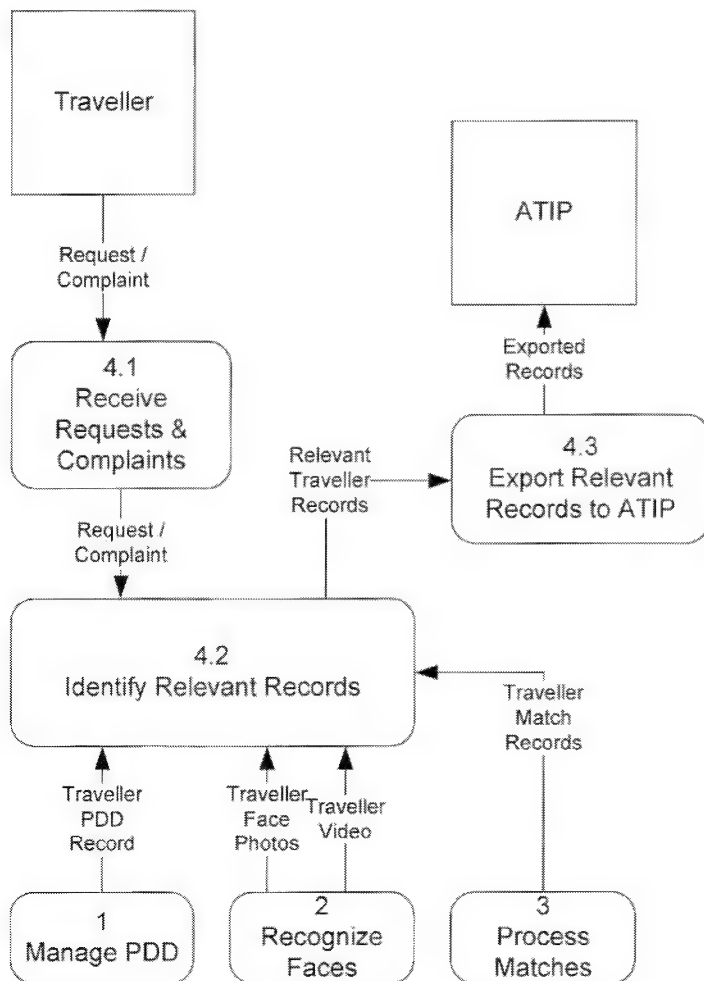


Figure 7: Data Flow Diagram - Process Requests & Complaints

If a traveller makes a formal access-to-information request or files a complaint with respect to the information gathered by the *FOTM* system within 30 days of the creation of a live-capture photo of the traveller (process 4.1), designated CBSA personnel will identify and retrieve from the system copies of records relevant to that traveller (process 4.2). Records could include PDD entries, face photos, video recordings, and match records. The relevant records will be copied to another storage medium such as a USB key or DVD and will be retained (process 4.3) for a minimum of two years in accordance with subsection 4(1) of the *Privacy Regulations*. All photo and PDD data and copies will be retained in accordance with the relevant CBSA security policy (Comptrollership Manual – Security Volume – Chapter 6: Storage of Sensitive Information and Assets). CBSA's ATIP division will handle the request or complaint from then on in accordance with its normal policies and practices. ATIP's process is beyond the scope of this system.

All live-capture photos (whether matched or not), operational and control PDD entries, match records (whether accepted or rejected by an adjudicator), and actor walkthrough records will be retained in

storage until the end of the project. This will allow in-demonstration and post-demonstration analysis of the FR technology's performance. The photo stream may be re-run several times against the PDD in a lab setting as matching parameters are adjusted to determine the optimal settings for minimizing false acceptance rates and false rejection rates. The match records, particularly for control subjects (actors), will be analyzed to assess the accuracy and effectiveness of the technology. This data will not be disclosed outside the CBSA (although statistics and experimental findings on the technology's readiness will be summarized in a final report). This use of photos, the PDD, the match records, and the walkthrough records is a non-administrative use. A non-administrative-use security protocol has been developed to address proper handling of this information.

All data within the system will be deleted or disposed of after the *FOTM* project ends. Disposal of all data will be done in accordance with the policy found in the CBSA Comptrollership Manual – Security Volume, Chapter 8: Disposal of Sensitive Information and Assets.

The photos and related data will be deleted or disposed of two years from the date that the last administrative action is taken with respect to it. Disposal of all data will be done in accordance with the policy found in the CBSA Comptrollership Manual – Security Volume, Chapter 8: Disposal of Sensitive Information and Assets.

All recordings and copies will be retained in accordance with the relevant CBSA security policy (Comptrollership Manual – Security Volume – Chapter 6: Storage of Sensitive Information and Assets).

Example of a Data Flow Model - Table

Source of the personal information for the program or activity

From whom or from what organization is the personal information collected? In other words, identify who is providing the personal information that is being used, will be used or available for use for the program or activity. There may be more than one source, indicate all sources:

SOURCE	IDENTIFY THE SOURCE
The individual or a representative	Only the individual.
A federal government institution (identify from what PIB the information is obtained)	Overt Audio-Video Surveillance (CBSA PPU 1104) CBSA Removals Program (CBSA PPU 1301)
Non-federal institutions	
- Provincial Government	N/A
- Municipal Government	N/A
- Aboriginal Government/ Council	N/A
- Organization of a Foreign State	N/A
- International Organization	N/A
Private Sector	
- Located in Canada and Canadian Owned	N/A

SOURCE	IDENTIFY THE SOURCE
- Located in Canada and Foreign Owned	N/A
- Located abroad and Canadian Owned	N/A
- Located abroad and Foreign Owned	N/A

Internal Use and Disclosure

Where will that information circulate within the federal government institution? This must identify any related programs or activities and personal information banks as identified in the institution's Info Source chapter.

Program	Personal information bank
Ports of entry	CBSA PPU 1104; CBSA PPU 1301
Investigations	CBSA PPU 026
Intelligence	N/A
Inland Enforcement	CBSA PPU 020, CBSA PPU 026, CBSA PPU 1301

External Use and Disclosure

Where will that information circulate outside of the federal government institution? This includes any disclosure made to:

The individual or a representative	An individual or his/her representative may make an ATIP request with respect to his/her information.
A federal government institution	Records may be disclosed within CBSA for the purpose of enforcing federal legislation.
Non-federal institutions and private sector	
- Provincial Government	N/A
- Municipal Government	N/A
- Aboriginal Government/ Council	N/A
- Organization of a Foreign State	N/A
- International Organization	N/A
Private Sector	
- Located in Canada and Canadian Owned	Records will be disclosed to Face4 Systems, a private-sector organization that will assist the CBSA in analyzing and evaluating the FR technology during the project. Face4 will work with CBSA ISTB personnel to re-run the live-capture photos against the PDD and

For Internal Use Only – Distribution Limited to Project Personnel

Faces on the Move: Multi-camera Screening

PIA

	<p>compile statistical information about true matches, false acceptances, and false rejections. They will modify system parameters that govern the matching processes to attempt to lower the false acceptance and false rejection rates as much as possible. Such disclosures will be made only for the purpose of assessing the performance of the technology. Such disclosures will only be made in accordance with the relevant legislative provisions and within the bounds of a clearly articulated contract.</p> <p>Note: ÉTS will not have access to personal information but will have access to derived information (scores of matches). They have no access to any of the match data, FOSS ID, photos, etc.</p>
- Located in Canada and Foreign Owned	N/A
- Located abroad and Canadian Owned	N/A
- Located abroad and Foreign Owned	N/A

Retention / Storage

Where will the information be stored or retained (identify all organizations that will store the information – this includes duplicates of the databases containing the personal information or any back-ups):

A federal government institution – within the CBSA	<p>Records will be stored at the location where they are made. The records will be housed on secure servers and in secure storage with access controls. When the live demonstration phase of the project is complete, all computing equipment, including storage devices and the records stored on them, will be moved to the CBSA's Science and Technology lab in Ottawa. The records will continue to be housed on the secure servers and in secure storage with access controls.</p> <p>In all cases where storage devices are used, they will be required to meet baseline physical security requirements based on the level of sensitivity of information gathered as per CBSA Security Volumes, depending on the recording medium.</p> <p>In cases where <i>FOTM</i> results in action being taken with respect to a matched traveller, relevant records will be exported to alternate systems or storage within CBSA. All such storage will comply with all security and privacy requirements.</p> <p>Records will not be disclosed to other federal government institutions.</p> <p>All personal information collected and held by the CBSA during this project will be deleted or disposed of at the end of the project in accordance with CBSA policies and procedures.</p>
A Federal Records Center	N/A

For Internal Use Only – Distribution Limited to Project Personnel

Faces on the Move: Multi-camera Screening

PIA

Non federal institutions and private sector	
1. Provincial Government	N/A
2. Municipal Government	N/A
- Aboriginal Government/ Council	N/A
- Organization of a Foreign State	N/A
- International Organization	N/A
Private Sector	
3. Located in Canada and Canadian Owned	N/A
4. Located in Canada and Foreign Owned	N/A
- Located abroad and Canadian Owned	N/A
- Located abroad and Foreign Owned	N/A

Other Possible Considerations

Identify the areas, groups and individuals who access and handle the personal information:

Identify the areas / groups / divisions who are allowed to access and handle the personal information collected for the program or activity. Also, identify where these areas or groups are located (i.e. national capital region, within a province, in a foreign country, or several locations if teleworking) as well as the location of the personal information to uncover any potential trans-border or inter-jurisdictional issues. When reasonable to do so, by virtue of the size of the organization or the number of individuals, identify individual positions rather than the work area or group.

Federal government Institution responsible for program or activity: Canada Border Services Agency		
Identify Groups or Areas / or Divisions	Positions who have access or use the personal information (where appropriate)	Geographical Location
Ports of entry	Chiefs, Supervisors and select Border Service Officers have access as part of their official duties.	The CBSA will deploy this system at the international arrivals hall and related areas at Pearson International Airport, Terminal 3.
Inland Enforcement Division	Chiefs, Supervisors and Investigation Officers have access as part of their official duties.	The CBSA will deploy this system at the international arrivals hall and related areas at Pearson International Airport, Terminal 3.

For Internal Use Only – Distribution Limited to Project Personnel

Faces on the Move: Multi-camera Screening

PIA

Science and Technology	Research scientists	The CBSA will move the system and all its data to the Science and Technology Lab in Ottawa for post-demonstration analysis.
Other federal government Institution responsible for program or activity: (one table per institution):		
N/A		
Non Federal Institution or Private Sector: Face4 Systems: (one table per institution)		
Face4 Systems	Technicians, technologists, system analysts, developers	Face4 Systems will manage the system remotely from the CBSA Science and Technology Lab in Ottawa. They will also conduct post-demonstration analysis of the system and the data it collected, also at the CBSA's Ottawa lab.

SECTION 7 - PRIVACY COMPLIANCE ANALYSIS

Legal Authority for Collection of Personal Information

Has a legal authority been identified for the collection of personal information for this program or activity?

Statutory reference: Section 4 of *Privacy Act* (Section 4 has been interpreted to mean that a legal authority must be established for a collection of personal information, but section 4 does not provide legal authority for such a collection).

Policy reference: Section 6.2.6 of *Directive on Privacy Practices*

Yes

- 1.1 ☒ Please specify the legal authority and briefly explain its connection to the program or activity or how it permits the collection of the personal information:

Immigration and Refugee Protection Act, paragraphs 15(1), 16(1), 16(1.1), 16(2), 16(2)(a), 16(2)(b), 16(2.1), 16(3), 18(1), and 18(2)

If legal authority is unclear consult your Legal Service to determine authority for the program or activity.

The CBSA's demonstration of FR is directly related to the cited paragraphs of the *IRPA*, which require all persons seeking entry to Canada to submit to an examination of their persons and documents. These paragraphs also allow for the presentation of photographic evidence of an applicant's identity.

Immigration and Refugee Protection Regulations, paragraphs 28, 28(a), 28(b), 28(c), and 28(d)

The cited regulations clarify that any person seeking to enter Canada is making an application under the terms of paragraphs 15 and 16 of the *IRPA*.

- 1.2 ☒ AND, ensure that the legal authority to collect the personal information is cited in the relevant PIB and in "Section I – Overview and PIA Initiation" of the PIA.

→ Continue to Question 2

No

- 1.3 ☐ If there is no legal authority for the collection of personal information, it cannot be collected. Please consult your institution's legal advisors to determine if there is authority to proceed with the program or activity.

Necessity to Collect Personal Information

Is each element and sub-element of personal information collected or to be collected necessary to administer the program or activity?

Statutory reference: Section 4 of *Privacy Act*

Policy reference: Sections 6.1.1, 6.1.3, 6.1.4, 6.2.7 and 6.2.8 of *Directive on Privacy Practices*

YES

- 2.1 ☒ Ensure that all personal information necessary to administer the program or activity is listed in the relevant PIB.

- 2.2 ☒ AND, implement controls and procedures to ensure the institution does not collect more personal information than is necessary for the identified program or activity and that a continuing need exists for that information or its collection.

→ Continue to Question 3

NO

- 2.3 ☐ Review the proposed elements and sub-elements of personal information outlined in "Section 3 – Analysis of Personal Information Elements" to identify those that are "necessary" and not merely useful. Document any changes.

Authority for the Collection, Use or Disclosure of the Social Insurance Number

Is the collection of the Social Insurance Number (SIN) necessary to administer the program or activity?

Statutory reference: Section 4 of Privacy Act

Policy reference: Section 6.2.13 of Policy on Privacy Protection and sections 6.1.1 and 6.2 to 6.4 of Directive on Social Insurance Number

Also see "Guidance for Preparing Information-Sharing agreements Involving Personal Information" and "Taking Privacy into Account Before making Contracting Decisions"

YES

- 3.1 ☐ Collection of the SIN must be in compliance with the Directive on Social Insurance Number (please check all appropriate boxes below):
- 3.2 ☐ State legal authority for collecting the SIN:

OR, in the absence of a legal authority to collect the SIN:

- 3.3 ☐ Establish explicit authority through legislative amendment(s).
- 3.4 ☐ Establish legal authority as outlined in the Directive on Social Insurance Number.

AND, if disclosure of the SIN by the institution is to occur on a routine or systematic basis

- 3.4.1 ☐ to another federal institution that is authorized to collect it, or to another level of government, establish an agreement or arrangement that includes specific provisions to limit the use of the SIN.
- 3.4.2 ☐ to a contractor or other external service provider, establish a contract that includes specific provisions to limit the use of the SIN.
- 3.5 ☐ AND, ensure that the relevant PIB for the program or activity states the authority under which the SIN is collected and the purpose for which it is used.

→ Continue to Question 4

NO

- 3.6 ☒ The SIN is not necessary and it will not be collected, used or disclosed to administer the program or activity.

→ Continue to Question 4

Direct Collection - Notification and Consent (as appropriate)

Is personal information collected directly from the individual to whom it relates?

Statutory reference: Sections 4 and 5 of Privacy Act

Policy reference: Sections 6.1.1, 6.2.6 and 6.2.9 to 6.2.13 of Directive on Privacy Practices and section 6.1.2 and 6.4.1 of Directive on Social Insurance Number

YES

- 4.1 ☒ A "Privacy Notice" (adapted for either verbal or written communications) must be provided to the individual at the time of collection and it must notify the individual of any of the following elements that apply (please check all appropriate boxes):
- ☒ a) The purpose and authority for the collection
 - ☒ b) Any uses or disclosures that are consistent with the original purpose.
 - ☐ c) Any uses or disclosures that are not related to the original purpose
 - ☐ d) Any legal or administrative consequences for refusing to provide the personal information
 - ☐ e) That the "individual to whom the information relates" has rights of access to, correction of and protection of personal information under the Privacy Act.
 - ☐ f) A reference to the PIB for the program or activity
 - ☐ g) Why the SIN is collected, how it will be used and the consequence of not providing it.

AND, add a "Consent Statement" to the "Privacy Notice" as appropriate, if the personal information is to be used or disclosed for a purpose other than the original purpose or a consistent use, or, to authorize indirect collection of personal information.

- 4.2 ☐ The "Consent Statement" must include, as applicable, the following elements (please check all appropriate boxes):
- ☐ a) The purpose of the consent and the specific personal information involved.
 - ☐ b) In the case of indirect collections, the sources that will be asked to provide the information.
 - ☐ c) Uses and disclosures that are not consistent with the original purpose of the collection and for which consent is being sought.
 - ☐ d) Any consequences that may result from withholding consent.
 - ☐ e) Any alternatives to providing consent

- 4.3 ☐ AND, implement controls and procedures to ensure that the institution keeps a record documenting whether or not an individual provided consent when it was sought, including a record documenting any withdrawal of consent when applicable.

→ Continue to Question 5

NO

- 4.4 ☐ The personal information necessary for the program or activity is not collected directly from the individual. It is collected indirectly, for example, from another program within the institution, or from another institution, government or third party.

→ Continue to Question 5

Indirect Collection - Consent or Authority under Sec. 10 of Privacy Regulations

Is personal information collected indirectly from another source with the informed consent of the individual to whom it relates, or from a person authorized to act on behalf of the individual pursuant to section 10 of the Privacy Regulations?

Statutory reference: Sections 4 and 5 of Privacy Act and section 10 of Privacy Regulations

Policy reference: Sections 6.1.1, 6.2.6 and 6.2.9 to 6.2.13 of Directive on Privacy Practices and sections 6.1.2 and 6.4.1 of the Directive on Social Insurance Number

YES

- 5.1 ☐ The notice and consent requirements stated at Question 4 apply. Please review the required elements listed under "YES" at Question 4 and check the corresponding boxes below to indicate the elements that need to be included in the "Privacy Notice" or the "Consent Statement" (check all that apply):

Privacy Notice	a) <input type="checkbox"/>	b) <input type="checkbox"/>	c) <input type="checkbox"/>	d) <input type="checkbox"/>	e) <input type="checkbox"/>	f) <input type="checkbox"/>	g) <input type="checkbox"/>
Consent Statement	a) <input type="checkbox"/>	b) <input type="checkbox"/>	c) <input type="checkbox"/>	d) <input type="checkbox"/>	e) <input type="checkbox"/>		

- 5.2 ☐ AND, implement controls and procedures to ensure the institution keeps a record documenting whether or not an individual provided consent when it was sought, including a record documenting any withdrawal of consent when applicable.
- 5.3 ☐ AND, if information is being collected from persons authorized to act on behalf of minors, incompetents or individuals who have been deceased for less than 20 years, implement appropriate mechanisms to ensure that such persons are authorized to act on behalf of individuals who do not have the capacity to provide consent.

→ Continue to Question 6

NO

- 5.4 ☒ → Continue to Question 6

Indirect Collection - Without Notification and Consent

Is personal information collected from another source without notice to or consent from the individual to whom the information relates?

Statutory reference: Sections 4, 5, 7 and 8 of Privacy Act and section 10 of Privacy Regulations

Policy reference: Sections 6.2.6 and 6.2.9 to 6.2.13 of Directive on Privacy Practices, section 6.2.15 of the Policy on Privacy Protection and sections 6.3.2 and 6.3.3 of Directive on Privacy Impact Assessment

YES

- 6.1 ☒ Where information is collected indirectly under any of the following circumstances without notice to, or consent from, the individual to whom it relates, please check the applicable boxes and explain as requested:
- ☒ a) The collection is a result of a disclosure to the institution under subsection 8(2) of the Privacy Act. State the applicable paragraph(s) of subsection 8(2) and provide a brief explanation for each:

The CBSA will disclose previously collected information to populate the PDD as permitted by 8(2)(a) of the Privacy Act. The PDD is used for a purpose consistent with

the original collection, namely enforcing compliance with sections 15(1), 16(1), 16(1.1), 16(2), 16(2)(a), 16(2)(b), 16(2.1), 16(3), 18(1), and 18(2) of the *Immigration and Refugee Protection Act* and sections 28, 28(a), 28(b), 28(c), and 28(d) of the *Immigration and Refugee Protection Regulations*.

- ☒ b) Direct notification of the individual might result in the collection of inaccurate information, or might defeat the purpose or prejudice the use for which the information is collected. Briefly explain why notice is not provided

If previously deported persons become aware that their faces are being photographed specifically for FR and that this is occurring only at Terminal 3 of Pearson International Airport, those persons may arrange to arrive at a different POE to avoid the FR or they may try to defeat the technology through head position, hats, glasses, etc.

- ☐ c) The information involved in the program or activity is to be used solely for a non-administrative purpose in which no decisions are made about the individuals to whom the information relates.

6.2 ☒ AND, if any of the circumstances in a) b) or c) is applicable, ensure that it is reflected in the relevant PIB.

6.3 ☐ AND, if the information is to be used solely for a non-administrative purpose (box c above has been checked), ensure that the requirements under sections 6.3.2 and 6.3.3 of the *Directive on Privacy Impact Assessment* have been met, and that the decision of the official responsible for section 10 of the *Privacy Act* to proceed with a PIA for the program or activity has been adequately documented in the description of the program or activity in "Section I - Overview and PIA Initiation" of the PIA.

6.4 ☐ OR, if none of the circumstances in a) b) or c) is applicable, then the personal information must be collected directly from the individual, or indirectly with the consent of the individual. Please review the responses to Questions 4 and 5 and ensure that the "Privacy Notice" or the "Consent Statement" includes all of the required elements listed under "YES" at Question 4.

→ Continue to Question 7

NO

6.5 ☐ All personal information is collected directly from the individual to whom it relates, or from another source with notice to, or consent from, the individual or a person authorized to act on behalf of the individual (see Questions 4 and 5 above).

→ Continue to Question 7

Retention and Disposal of Personal Information

Has Library and Archives Canada approved a records retention and disposal schedule that applies to the personal information?

Statutory reference: Section 12 of *Library and Archives Canada Act*, sections 6, 10 and 11 of *Privacy Act* and section 4 of *Privacy Regulations*

Policy reference: Sections 6.1.3, 6.2.11 to 6.2.13 and 6.2.23 of *Directive on Privacy Practices*

YES

7.1 ☒ Please identify the Record Disposition Authority (RDA) and describe the retention and

disposal schedule:

For any record considered to be a transitory record, the RDA is MIDA 90/000: transitory records will be retained until the end of the project and will be destroyed within 15 days of the expiration of that retention period.

Recordings of FR activity that are used to obtain or provide information or to investigate an allegation or complaint, or used as evidence in respect of an identifiable individual shall be kept for the longer of two (2) years following the date of their creation, or following the date of their last use in an administrative action as information or as evidence in respect of that person.

A RDA has been requested from Library and Archives Canada for all records which are not considered to be transitory. The request has not yet been approved; however it is the intention of the CBSA to retain these records in accordance with paragraph 4(1)(a) of the *Privacy Regulations*, for a minimum of two years from the date of their creation.

- 7.2 ☒ AND, implement controls and procedures to ensure that personal information used to make a decision that directly affects an individual will be retained for a minimum of two years after the last administrative action or, where a request for access to the information has been received, until such time as the individual has had the opportunity to exercise all his/her rights under the Act)
- 7.3 ☐ AND, if the institution intends to dispose of personal information that has been used for an administrative purpose prior to the expiration of the two-year minimum retention standard established by the *Privacy Regulations*, it must obtain the consent of the individual to whom the information relates before doing so.

- 7.4 ☒ AND, the institution must cite the RDA number, the retention period and the disposition standards for the personal information in the relevant PIB.

→ Continue to Question 8

NO

- 7.5 ☒ Provide a Records Disposition Submission to Library and Archives Canada describing the records containing the personal information for which the institution requires a RDA.
The CBSA has requested a RDA for all audio-video records that are not considered to be transitory.

- 7.6 ☒ AND, obtain a RDA from Library and Archives Canada to allow the institution, under certain conditions, to dispose of records that no longer have operational utility for the program or activity.

- 7.7 ☒ AND, ensure that all the other applicable requirements listed under "YES" at Question 7 are met.

→ Continue to Question 8

Accuracy of Personal Information

Will measures be adopted to ensure that personal information used by the institution for an administrative purpose is as accurate, up-to-date and complete as possible?

Statutory reference: Sections 6, 10 and 11 of *Privacy Act* and sections 10 and 11 of *Privacy Regulations*

Policy reference: Sections 6.1.1 and 6.2.9 to 6.2.16 of Directive on Privacy Practices

YES

- 8.1 ☒ Please check any of the following measures that will be adopted to ensure accuracy of the personal information and provide details as requested:
- 8.1.1 ☒ Personal information will be collected directly from the individual to whom it relates or it will be validated with the individual or a person authorized to act on behalf of the individual.
- 8.1.2 ☐ A data-matching process will be used to verify the accuracy of personal information against a "reliable source" (within or outside the institution) where this is authorized, or where consent was obtained. Please briefly describe the data-matching process and the source(s) that will be used to ensure accuracy of the information:
-
- 8.1.3 ☒ In cases where direct collection or consent is not feasible, the institution will obtain information from trusted sources (public or private) and verify accuracy against existing personal information before use. Please identify the sources and procedures to be used to check the accuracy of the information:
- Information for the PDD will be collected from existing CBSA sources, which are deemed to be accurate at the time of collection.
- 8.1.4 ☐ Technological methods will be used to identify errors and discrepancies. Please briefly describe these technological methods:
-
- 8.1.5 ☐ Other – please specify:
-
- 8.2 ☒ AND, if measures are adopted other than "*direct collection or validation with the individual or with a person authorized to act on behalf of the individual*", the institution must implement appropriate controls and procedures to ensure that:
- a) the technique(s) and the specific source(s) used to validate or update the personal information are documented;
 - b) individuals are given the opportunity, whenever possible, to request correction of any inaccurate personal information before the information is used in a decision-making process that affects them;
 - c) personal information can only be modified or corrected by those within the institution who have the authority to do so; and
 - d) when personal information is corrected or annotated, other authorized holders of the information are notified about the correction or annotation and that all copies of the information in the possession of the institution are corrected / annotated.

- 8.3 ☐ AND, if appropriate, ensure that the “Privacy Notice” or “Consent Statement” and the relevant PIB are amended to identify the data-matching activity including the source(s).

→ Continue to Question 9

NO

- 8.4 ☐ Please explain why such measures will not be adopted:

→ Continue to next Question 9

Use of Personal Information

Will the personal information collected for the program or activity be used solely for the original purpose for which it was obtained or compiled, a use consistent with that purpose, or a purpose for which the information was disclosed to the institution pursuant to subsection 8(2) of the Privacy Act?

Statutory reference: Sections 5 and 7 to 11 of Privacy Act

Policy reference: Sections 6.1.1, 6.1.9, 6.2.9 to 6.2.13 and 6.2.17 of Directive on Privacy Practices, section 6.2.15 of Policy on Privacy Protection and Section IV of Appendix C of Directive on Privacy Impact Assessment

YES

- 9.1 ☒ Implement controls and procedures to ensure that access to the personal information for such purposes will be limited to authorized individuals who need to know the information to perform their official duties
- 9.2 ☒ AND, ensure that the “Data Flow Diagram” or “Data Flow Tables” completed for “Section IV – Flow of Personal Information” of the PIA identify the areas, groups and individuals (e.g., the positions) within the institution who have a need-to-know to access to or handle the personal information, including their geographical location and where the personal information will be stored or retained.
- 9.3 ☒ AND, if the purposes for which the personal information is used includes any use(s) of the information for a non-administrative purpose, (such as research, statistical, audit and evaluation purposes) the institution will adhere to the requirements and principles in its “**Privacy Protocol For Non-Administrative Purposes**”, in accordance with section 6.2.15 of the Policy on Privacy Protection, to address any impact that such non-administrative uses may have on privacy.

→ Continue to Question 10

NO

- 9.4 ☐ Identify below any other uses of the personal information, in other words, any routine uses that are not directly related to the purpose of the collection, or, which are not consistent with that purpose or for which the information was disclosed to the institution pursuant to subsection 8(2) of the Privacy Act:

- 9.5 ☐ AND, ensure that these other uses are reflected in the relevant PIB

- 9.6 ☐ AND, include a description of these other uses in the “Privacy Notice” or “Consent Statement”, as appropriate,
☐ AND, ensure the all the other applicable requirements listed under “YES” at Question 9 are met.
 → Continue to Question 10

Disclosures Directly Related to the Administration of the Program or Activity

Will personal information be disclosed for purposes directly related to the administration of the program or activity?

Statutory reference: Sections 5 and 8 to 11 of *Privacy Act*.

Policy reference: Sections 6.2.10, 6.2.11 and 6.2.13 of *Policy on Privacy Protection*, sections 6.2.1 to 6.2.3 of *Directive on Social Insurance Number*, sections 6.1.9, 6.2.9 to 6.2.13 and 6.2.15 to 6.2.20 of *Directive on Privacy Practices* and section IV of Appendix “C” of *Directive on Privacy Impact Assessment*)

Also see “Guidance for Preparing Information-Sharing agreements Involving Personal Information” and “Taking Privacy into Account Before making Contracting Decisions

YES

- 10.1 ☒ Please check all applicable boxes below and, for each disclosure, identify the name of the organization or third party to which personal information will be disclosed. If it is disclosed within the institution, please identify the branch and the program or activity.
- 10.1.1 ☒ Within the institution for another program or activity – specify
 IED
- 10.1.2 ☐ Other federal government institutions – specify
- 10.1.3 ☐ Provincial, territorial or municipal governments institutions – specify
- 10.1.4 ☐ Foreign government institutions and entities thereof – specify
- 10.1.5 ☐ International organizations – specify
- 10.1.6 ☒ The private sector (e.g., contractor or other external service provider) – specify
 • Face4 Systems, a contractor that is assisting in the deployment, management, maintenance, and post-demonstration analysis of the system.
- 10.1.7 ☐ Other – specify

10.2 ☒ AND, ensure that:

- a) any such disclosure is made in compliance with section 8 of the *Privacy Act*, which allows disclosures of personal information with consent of the individual to whom the information relates (subsection 8(1)) or without consent in certain and limited circumstances pursuant to subsection 8(2) of the Act;
- b) only personal information elements that are necessary for the intended purpose are disclosed;
- c) the organization or third party receiving the personal information is authorized to do so;
- d) administrative, physical and technical safeguards appropriate to the sensitivity of the information will be applied to protect the information during and after its transmission (see Question 15);
- e) the organization or third party to which the personal information will be disclosed for the administration of the program or activity are identified in the "Consistent Use" section in the relevant PIB in *Info Source*, including the specific purpose of the disclosure;
- f) the "**Privacy Notice**" or "**Consent Statement**" describes any disclosures of information; and,
- g) the "Data Flow Diagram" or "Data Flow Tables" completed in "*Section IV – Flow of Personal Information*" of the PIA include details on the disclosed personal information:

10.3 ☒ AND, any disclosure of personal information to another federal institution or outside the Government of Canada is governed by a formal agreement or arrangement (e.g., a Memorandum of Understanding, an accord, a contractual arrangement, etc.) to ensure that appropriate privacy protection clauses are included, and, where applicable, include provisions for inter-jurisdictional or trans-border flows of personal information. Such clauses must cover the following topics:

- a) Control over personal information, where appropriate.
- b) Limitations on the collection, retention, use and disclosure of personal information.
- c) Measures (administrative, technical and physical) to protect the integrity and confidentiality of personal information.
- d) Measures governing the disposition of the personal information, where relevant
- e) Measures to ensure or verify that the personal information is only used for the purposes related to the agreement, arrangement or contract.
- f) Obligations are to be extended to other parties such as subcontractors.

→ Continue to Question 11

NO

10.4 ☐ There is no disclosure of personal information within or outside the institution for purposes that are directly related to the administration of the program or activity.

→ Continue to Question 11

Accounting for New Uses or Disclosures Not Reported in Info Source

Will controls and procedures be implemented to account for any new use or disclosure of the personal information that is not included in the relevant PIB published in Info Source?

Statutory reference: Sections 7 to 11 of Privacy Act and section 4 of Privacy Regulations

Policy reference: Sections 6.1.9 and 6.2.2 of Directive on Privacy Practices

YES

11.1 ☒ Appropriate controls and procedures have been or will be implemented to ensure that:

- a) the head of the institution or the appropriate delegate is notified about any new use or disclosure of personal information that is not reflected in the PIB description published in *Info Source*;
- b) the consent of the individual to whom the information relates is obtained in writing, as appropriate, prior to any new use of the information for an administrative purpose that is not reflected in the relevant PIB published in *Info Source*, unless the new use is considered to be consistent with the purpose for which the personal information was obtained or compiled and the Privacy Commissioner is notified forthwith regarding the new consistent use;
- c) except as permitted under subsection 8(2) of the Privacy Act, any disclosure of personal information for a purpose that is not reflected in the relevant PIB published in *Info Source* will only be made with the consent of the individual to whom the information relates;
- d) a record is kept for any new use or disclosure of personal information not described in the relevant PIB published in *Info Source*, and that this record is stored with the personal information to which it relates and retained for a minimum period of two years following such a use or disclosure
- e) if the information is disclosed to a federal investigative body under paragraph 8(2)(e) of the Privacy Act, the record of disclosure will be kept in a separate PIB for a period of two years where it will be available to the Privacy Commissioner for review upon request;
- f) the Privacy Commissioner is notified forthwith, as required under subsection 9(4) of the Act, of any new use or disclosure that is consistent with the purpose for which the information was obtained or compiled, but which is not reflected in the relevant PIB published in *Info Source*;
- g) the relevant PIB is amended in time for the next edition of *Info Source* to include any new use(s) or disclosure(s) that are consistent with the purpose for which the information was obtained or compiled, as well as any routine use(s) or disclosure(s) that do not fall within the categories of purpose of collection or consistent use; and
- h) the Privacy Commissioner is notified prior to or forthwith, as required under subsection 8(5) of the Act, about any disclosures made or to be made in the public interest or in the interest of the individual to whom the information relates.
- i) Other, specify

→ Continue to Question 12

NO

- 11.2 ☐ Please explain why such controls and procedures will not be implemented (provide adequate justification):

→ Continue to Question 12

Safeguards – Statement of Sensitivity

Has a Statement of Sensitivity (SoS) or similar analysis been completed to assess the degree of sensitivity of the personal information to be collected and retained for the program or activity?

Statutory reference: Sections 7 and 8 of Privacy Act.

Policy reference: Appendix C of Directive on Privacy Impact Assessment and sections 6.2.17 to 6.2.21 of Directive on Privacy Practices, Policy on Government Security, Operational Security Standard: Management of Information Technology Security (MITS)

YES

- 12.1 ☒ The information contained in the SoS or similar analysis has been taken into account when assessing the level of risks to privacy in "Section 2 - Risk Area Identification and Categorization" of the PIA.

→ Continue to Question 13

NO

- 12.2 ☐ Please explain why a SoS or similar analysis was not considered necessary to assess the sensitivity of the information.

→ Continue to Question 13

Safeguards - Threat and Risk Assessment

Has a Threat and Risk Assessment (TRA) or a similar security assessment been completed for the program or activity?

Statutory reference: Sections 7 and 8 of Privacy Act.

Policy reference: Appendix C of Directive on Privacy Impact Assessment and sections 6.2.17 to 6.2.21 of Directive on Privacy Practices, Policy on Government Security, Operational Security Standard: Management of Information Technology Security (MITS)

YES

- 13.1 ☐ Reference the title of the TRA or other security assessment in "Section VII – Supplementary Documents List" and provide a brief synopsis of the assessment in the space below:

- 13.2 ☐ AND, obtain assurances from the officials responsible for the program or activity that the measures recommended in the assessment have been implemented to ensure the confidentiality, availability and integrity of the personal information.

- 13.3 ☐ AND, ensure that any residual risks to personal information are known and accepted by the executive or senior official responsible for the program or activity and the Head or delegated authority for the *Privacy Act*.

→ Continue to Question 14

NO

- 13.4 ☒ If a TRA or similar security assessment is underway, simply reference that fact in the space below and indicate when it is likely to be completed. If there is no intent to complete one, please explain.

A Security Assessment is underway. It cannot be completed until the system design is finalized. Initial review of the in-progress design is that this is generally a low-risk system, mainly because it is not connected to any other CBSA systems and because it will exist for only a limited time. Internet connectivity for remote management is noted and identified as a concern. The final design will include a VPN to protect this interface.

→ Continue to Question 14

Safeguards - Administrative, Physical and Technical

Please identify below any administrative, physical and technical safeguards in place, or to be implemented, for this program or activity to ensure the confidentiality, availability and integrity of the personal information.

Statutory reference: Sections 7 and 8 of *Privacy Act*

Policy reference: Appendix C of *Directive on Privacy Impact Assessment* and sections 6.2.17 to 6.2.21 of *Directive on Privacy Practices*, *Policy on Government Security*, *Operational Security Standard: Management of Information Technology Security (MITS)*

Please check all that apply, including safeguards identified by the TRA or similar security assessment.

14.1 Administrative safeguards

- ☒ Internal security and privacy policies and procedures
- ☒ Staff training on privacy and the protection of personal information
- ☒ Screening and security checks of employees
- ☒ Appropriate security levels for employees who will have access to personal information
- ☒ Contingency plans and documented procedures in place to identify and respond to security and privacy breaches
- ☐ Regular monitoring of users' security practices
- ☒ Methods to ensure that only authorized personnel who need to know have access to personal information
- ☐ Other – please describe

14.2 Physical safeguards

- ☒ Restricted access areas
- ☐ Security guards
- ☒ Identification badges are worn by staff at all times
- ☒ After hours alarms and monitoring systems
- ☒ Locked filing cabinets
- ☐ Combination locks
- ☒ Safes
- ☐ Cipher locks
- ☒ Key cards
- ☒ Video surveillance (closed-circuit television)
- ☒ Secured server locations
- ☐ Backups secured off-site
- ☐ Other – please describe

14.3 Technical safeguards

- ☒ Role-based user authorization and authentication
- ☐ Biometrics
- ☒ Passwords (minimum of 6 characters long, include alpha and numeric characters)
- ☐ Passwords are changed by users every 90 days and recently used passwords cannot be re-used)
- ☐ Password protected screensavers
- ☒ Session-time out security (automatically locks an account after a session has been idle for a specified amount of time)
- ☒ Firewalls
- ☒ Intrusion Detection System (IDS)
- ☒ Virtual Private Network (VPN)
- ☒ Encryption of sensitive information
- ☐ Government of Canada Public Key Infrastructure Certificates (PKI)
- ☐ External Certificate Authority (CA)
- ☒ Audit trails
- ☐ Other – please describe

→ Continue to Question 15

Technology and Privacy - Tracking Technologies

Will the information system(s) used to deliver the program or activity employ cookies or other tracking technologies to collect personal information about users and their transactions?

Statutory reference: Sections 4 to 10 of the Privacy Act and section 4 of Privacy Regulations

Policy reference: Subsections 6.1.1, 6.1.3, 6.1.9, 6.2.9 to 6.2.13, 6.2.17 and 6.2.23 of Directive on Privacy Practices

YES

- 15.1 ☐ The specific tracking technologies to be used is adequately described under Part F: Technology and Privacy of "Section II – Risk Area Identification and Categorization" of the PIA;
- 15.2 ☐ AND, the collection of any personal information using such technologies is reflected in the relevant PIB and in "Section III – Analysis of Personal Information Elements" of the PIA;
- 15.3 ☐ AND, the use of such technologies to collect information about users and their transactions is adequately reflected in the "Privacy Notice";
- 15.4 ☐ AND, those responsible for implementing and using tracking technologies to collect personal information or who may have access to personal information collected through these methods are made aware of privacy and security policy requirements;
- 15.5 ☐ AND, where personal information collected through such tracking technologies is used to make a decision that directly affects the individual to whom the information relates, it will be retained for a minimum of two years after the last administrative action as required under the Privacy Regulations.

→ Continue to Question 16

NO

- 15.6 ☒ Tracking technologies are not used to collect personal information about users.

→ Continue to Question 16

Technology and Privacy - Surveillance or Monitoring

Will the new or modified program or activity result in new or increased surveillance or monitoring of a targeted population?

Statutory reference: Sections 4 to 10 of Privacy Act, section 4 of Privacy Regulations and section 8 of the Charter of Rights and Freedoms

Policy reference: Subsections 6.1.1, 6.1.9, 6.2.9 to 6.2.13 and 6.2.17 of Directive on Privacy Practices

YES

- 16.1 ☒ Consult with your legal advisors to determine whether or not such surveillance or monitoring activities raise any issues relating to the Charter of Rights and Freedoms, the Privacy Act or other applicable acts.
- 16.2 ☒ AND, ensure the surveillance or monitoring method(s) to be used, the characteristic(s) of the targeted population and the scope of the surveillance or monitoring are adequately described under Technology and Privacy of "Section II – Risk Area Identification and Categorization" of the PIA.
- 16.3 ☒ AND, any personal information collected or created as a result of such surveillance or

monitoring is described in the relevant PIB and in *Section III – Analysis of Personal Information Elements* of the PIA.

- 16.4 ☒ AND, the collection or use of personal information through surveillance or monitoring is adequately reflected in the "**Privacy Notice**", unless such notification might result in the collection of inaccurate information or defeat the purpose or prejudice the use for which the personal information is collected.

☐ If notice about surveillance or monitoring will not be provided, please explain why:

- 16.5 ☒ AND, those responsible for implementing and using such surveillance or monitoring method(s) or who may have access to personal information collected or created through these methods are made aware of privacy and security policy requirements.

→ Continue to Question 17

NO

- 16.6 ☐ The new or modified program or activity will not result in surveillance or monitoring.

→ Continue to Question 17

Considerations Related to Compliance, Regulatory Investigation, Enforcement

Does the program or activity involve compliance/regulatory investigation or law enforcement, surveillance or intelligence gathering that targets specific individuals against whom penalties, criminal charges or sanctions may be applicable?

Statutory reference: Sections 4 to 10 of *Privacy Act*, section 4 of *Privacy Regulations* and section 8 of the *Charter of Rights and Freedoms*

Policy reference: Subsections 6.1.1, 6.1.9, 6.2.9 to 6.2.13 and 6.2.17 of *Directive on Privacy Practices*

YES

- 17.1 ☒ Consult with your legal advisors to determine whether or not the compliance/regulatory investigation or law enforcement activities raise any issues relating to the *Charter of Rights and Freedoms*, the *Privacy Act* or other applicable acts.

- 17.2 ☒ AND, identify the legislative authority and the specific regulatory or law enforcement purpose involved:

The activity is undertaken in accordance with *Immigration and Refugee Protection Act*, paragraphs 15(1), 16(1), 16(1.1), 16(2), 16(2)(a), 16(2)(b), 16(2.1), 16(3), 18(1), and 18(2) and *Immigration and Refugee Protection Regulations*, paragraphs 28, 28(a), 28(b), 28(c), and 28(d).

- 17.3 ☐ AND, if the legislative authority differs from the legal authority for the program or activity, ensure it is adequately reflected in the response to Question 1 of "*Section V – Privacy Compliance Analysis*" and in "*Section I – Overview and PIA Initiation*" of the PIA.

- 17.4 ☒ AND, any personal information collected or created as a result of such regulatory or criminal enforcement, surveillance or intelligence gathering program or activity is described in the relevant PIB and in "*Section III – Analysis of Personal Information Elements*" of the PIA.

- 17.5 ☒ AND, the collection or use of personal information through these compliance / regulatory

For Internal Use Only – Distribution Limited to Project Personnel

Faces on the Move: Multi-camera Screening

PIA

investigation or enforcement activities is adequately reflected in the "Privacy Notice", unless such notification might result in the collection of inaccurate information or defeat the purpose, or prejudice the use, for which the personal information is collected.

- ☒ If notice about the compliance/regulatory investigation or law enforcement activities will not be provided, please explain why:

If previously deported persons become aware that their faces are being photographed specifically for FR in support of immigration enforcement and that this is occurring only at Terminal 3 of Pearson International Airport, those persons may arrange to arrive at a different POE to avoid the FR or they may try to defeat the technology through head position, hats, glasses, etc.

NO

- 17.6 ☐ The program or activity does not involve the conduct of regulatory or criminal enforcement, surveillance or intelligence gathering.

Note: The table below can be used to keep an account of actions completed and to track outstanding actions required to achieve privacy compliance:

Privacy Compliance Analysis question #	Action required to support legal and policy compliance (cross reference to relevant question of Section 5 – Privacy Compliance Analysis)	Done	To be done
1	Legal authority for the program has been established and is reflected in the relevant PIB.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2	a) The categories and elements of personal information to be collected for the new program have been carefully assessed based, for example, on the institution's experience gained with the administration of a similar program. The personal data collected will be limited to only that which is required.)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	b) These categories and elements of personal information have been described in the relevant PIB for the program.	<input type="checkbox"/>	<input checked="" type="checkbox"/>
	c) Controls and procedures will be implemented to ensure that the institution does not collect more personal information than necessary for the program and that a continuing need exists for that information and its collection.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
4 and 5	a) All of the requisite "Privacy Notices" and "Consent Statements" that meet the requirements of sections 6.2.9 to 6.2.12 of the <i>Directive on Privacy Practices</i> have been drafted. (Texts of the notices and consent statements may be included here.)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	The following notices are posted in Terminal 3 of Pearson International Airport:		

For Internal Use Only – Distribution Limited to Project Personnel

Faces on the Move: Multi-camera Screening

PIA

"This area is under video surveillance.

"Recordings may be used and shared in accordance with applicable federal legislation.

For more information on the CBSA's use of these recordings, please ask to speak with a supervisor or visit www.cbsa-asfc.gc.ca."

b) Controls and procedures have been implemented to keep records of individual consents, and to ensure that persons acting on behalf of individuals who do not have the capacity to provide consent have the authority to do so under section 10 of the *Privacy Regulations*.



7

a) A Records Disposition Authority (RDA) has been approved by Library and Archives Canada to authorize the disposal of the records containing personal information for the program.



b) Controls and procedures have been implemented within the program and the ATIP Office to ensure that information that has been used for an administrative purpose will be kept for the minimum retention period established by the *Privacy Regulations*.



c) Reference to the RDA, the retention period and the disposition standards for the program have been cited in the relevant PIB.



8

Controls and procedures are in the process of being implemented to ensure that the personal information associated with the program is as accurate, complete and up-to-date as necessary.



SECTION 8 - SUMMARY OF ANALYSIS AND RECOMMENDATIONS

Four-Part Test

The use of biometrics to screen travellers against an active database is highly visible and may be controversial if privacy risks and societal implications are not considered at the outset. Although the PIA identified the pressing societal need for identifying illegitimate travellers at the border, the effectiveness and proportionality of using FR to match against databases has not yet been fully evaluated; such an evaluation is the goal of the *Faces on the Move (FOTM)* project.

A number of scientific studies have tested the accuracy of biometrically enabled matching in a laboratory setting. However, the CBSA has not yet evaluated the performance of these algorithms in an operational environment. The CBSA is unsure if FR technology will be effective and therefore cannot evaluate the proportionality of FR screening without first conducting this project.

The technical demonstration project is designed to produce the necessary data with minimal infringements on individual privacy. The testing area is confined to a single terminal at Pearson International Airport. The environmental conditions within the terminal have been optimized for lighting conditions and camera placement to ensure that the quality of facial images minimize the likelihood of false positive matches. The system is configured to only match against individuals on the Previously Deported Persons list, who have already been determined to be inadmissible to Canada and have demonstrated their intent to return to Canada under a false name. Multiple points of human intervention have been created to ensure that any actions taken as a result of a positive match have been reviewed independently by a trained BSO. Finally, a positive real-time match will only result in a referral to secondary examination where standard procedures to establish the traveller's identity will be followed. These safeguards have been implemented in order to minimally impact privacy while still enabling the CBSA to evaluate the readiness of FR matching in an operational setting.

The CBSA recognizes that it could test the system on a control group of "actors" exclusively, thereby eliminating the use of "live" data. However, the control group may not have the desired heterogeneity in lighting, resolution, and diversity which is required to properly evaluate the effectiveness of FR screening technology. Testing the system using an operational database will also enable the CBSA to identify any weaknesses in the photograph enrolment process caused by poor lighting, low resolution, or facial obstructions. Excluding the use of operational data may appear to be a less privacy invasive means of demonstrating the solution, however, the CBSA believes the use of actors and "live" data in a narrowly controlled environment will allow the Agency to identify and mitigate privacy risks in the future.

Risk: Poor performance of FR technology may cause a disproportionate impact on traveller privacy.

Mitigation: The CBSA has implemented a number of measures to improve accuracy of the system including controlling environmental conditions, limiting the population of the PDD, introducing multiple points of human intervention, and processing only high-probability matches in real time.

Recommendation: The CBSA will conduct a new four-part test for any facial recognition screening program it may implement in the future.

ACCOUNTABILITY

Within the CBSA

The CBSA has a robust administrative structure to ensure compliance with the *Privacy Act* and related policies and directives. In FY 2012-2013, a Privacy Oversight Committee (PoC) was established which consists of senior-level executives within the CBSA that meet regularly throughout the year to discuss privacy issues, as well as monitor the development of privacy policy instruments and PIAs. The PoC also helps identify a need to assess upcoming initiatives for potential PIAs.

Bi-monthly reports on the status of PIAs are provided routinely to the PoC and the Office of the Privacy Commissioner to ensure adequate planning for the completion of PIAs. The FOTM project was presented to the PoC in March 2015.

The ATIP Division is responsible for recommending the development of a PIA and/or other measures to ensure that existing or new programs / activities are privacy compliant. When contacted, the ATIP Division will provide program areas with the Privacy Impact Questionnaire (PIQ). The PIQ is a template that requests high-level information similar to sections 1 and 2 of the Core PIA template, and is used to develop and record any recommendations given by the ATIP Division concerning the program or activity. The PIQ enables the ATIP Division to make informed recommendations as to whether or not a PIA or other privacy compliant measures are required.

The ATIP Division is also a required stakeholder in the development of Written Collaborative Arrangements (WCAs) such as Memorandums of Understanding or Information Sharing Agreements. Aside from reviewing WCAs for compliance with the *Privacy Act* and Treasury Board of Canada Secretariat policies, directives, and guidelines, the ATIP Division also makes recommendations with respect to the conduct of a PIA before the implementation of WCAs.

In FY 2012-2013, the CBSA also developed two privacy policy instruments:

- The Privacy Breach Protocol; and
- The Directive on Non-Administrative Uses of Personal Information (Privacy Protocol)

The Privacy Breach Protocol ensures that all security violations which include personal information are reported to the ATIP Division in addition to the Security and Professional Standards Division, and outlines the roles and responsibilities of the Agency with respect to privacy breaches, which may include notification of the individuals, notification of the Office of the Privacy Commissioner, and the identification of mitigating measures.

The Directive on Non-Administrative Uses of Personal Information sets out the process, roles and responsibilities for the creation of a Privacy Protocol for those programs and initiatives the use personal information for non-administrative purposes, such as statistical reporting.

In FY 2013-2014 the CBSA introduced an online awareness course on Information Management (IM) and Access to Information and Privacy (ATIP). The course was jointly developed in FY 2012-2013 and seeks to educate employees on their IM and ATIP responsibilities. This course will be supplemented by current training activities, which include an in-depth session on the administration of the ATIP program at the CBSA, the development of PIAs, and Info Source training.

Specific to the Faces on the Move Project

Personal information collected from the six month testing phase will be disclosed to Face4 Systems for evaluation after the testing period has concluded and the system has been removed from Pearson Airport. The contract between Face4 Systems and the CBSA outlines a number of safeguards for handling personal information, including a clear date for when all personal information under its control must be destroyed (project end). Face4 Systems originally intended to evaluate the FOTM project at their premises in Ottawa. However, upon reflection during the PIA process, the CBSA determined that granting Face4 Systems personnel access to the CBSA's SED lab would enable the Agency to exercise greater accountability for personal information collected under the project.

Risk: *Face4 Systems may not abide by the terms and conditions stipulated in the contract.*

Mitigation: *The CBSA will ensure that access to match data and all personal information by Face4 Systems staff will be limited to the CBSA's SED Lab, and will reflect control procedures in accordance with the Face 4 contract and the CBSA FOTM demonstration procedures that have been established for data collection and analyses.*

IDENTIFYING PURPOSES

Within the CBSA

The CBSA maintains its *Info Source* chapter on its website at <http://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/pia-efvp/atip-aiprp/infosource-eng.html>. It conducts ongoing reviews of the chapter to ensure that it accurately and completely describes the personal information activities of the Agency. The CBSA also ensures that appropriate Privacy Notice Statements are reflected on forms and websites, unless such notice is not required pursuant to sub-section 5(3) of the *Privacy Act*.

Specific to the Faces on the Move Project

CBSA PIB PPU 1104 (Overt Audio Video Surveillance) reflects the types of information collected, the purpose, legislative authority, and the consistent uses of information collected by CBSA video surveillance cameras. The PIB does not currently reflect the use of video surveillance cameras for the purpose of FR screening. The Records Disposition Authority (RDA) and Retention and Disposal Standard (RDS) have not yet been published; both are currently reflected in the PIB as "under development". However, personal information collected under the FOTM project will be subject to the retention period specified under the contract with Face4 systems.

Risk: CBSA PIB PPU 1104 (Overt Audio Video Surveillance) has not reflected a RDA or RDS in approximately two years. Moreover, if the FR solution were to be implemented or tested any further, the "Description" Section should include the personal information category of "biometric information". Also, the use of FR should be listed in the "consistent uses" section of the PIB.

Recommendation: The CBSA will update the RDA and RDS for CBSA PIB PPU 1104. The addition of "biometric information" and its use will be added to the "Description" and "Consistent Uses" section if biometric-based screening is considered for permanent deployment in the future.

The CBSA already collects Overt Audio-Video Surveillance as part of its normal port operations. Although the FOTM project was developed in compliance with the CBSA's *Policy on the Overt Use of Audio-Video Monitoring and Recording Technology*, the use of FR biometrics is not specifically identified within the Policy. The CBSA has chosen not to update the Policy at this time because the FOTM project is temporary and there are no plans to install this system permanently. At a minimum, the policy statements reflecting "permitted uses" would have to include FR. Also, additional guidance may also be necessary to ensure policy compliance.

Risk: The FOTM project is not integrated into the CBSA's *Policy on the Overt Use of Audio-Video Monitoring and Recording Technology*.

Recommendation: The CBSA should align the use of FR screening into the *Policy on the Overt Use of Audio-Video Monitoring and Recording Technology*. In the interim, the CBSA will ensure the FOTM project is managed in accordance with the Policy.

LIMITING USE, DISCLOSURE AND RETENTION

Within the CBSA

Throughout the PIA process, the ATIP Division works with program areas to ensure that CBSA programs limit the use, disclosure, and retention of personal information to only that which is necessary to administer the program or activity.

In FY 2012-2013, the CBSA developed guidelines on the disclosure of customs information pursuant to s.107 of the *Customs Act*. These guidelines set out the specific provisions, their limitations, relevant considerations and the appropriate positions within the CBSA (employee, supervisor, senior manager) that can authorize specific disclosures or uses. Personal information that is also customs information is disclosed in accordance with s.107 of the *Customs Act* rather than ss. 8(2) of the *Privacy Act*.

A similar set of guidelines for s. 8(2) of the *Privacy Act* was implemented in FY 2013-2014.

Specific to Faces on the Move Project

The original scope of the project included disclosure to municipal police in the event that an individual was matched to the system but had already cleared the Primary Inspection Line before they could be intercepted. However, the privacy risk of disclosing inaccurate information to another law enforcement organization was deemed to be disproportional, particularly outside of the context of reduced

expectation of privacy at the border. Further, the CBSA considered including additional databases to match against but chose to limit the use of the FOTM project to a subset of the Previously Deported Persons list exclusively for the purposes described above. Finally, carefully monitored retention schedules have been put into place to ensure that the program is “torn-down” at its conclusion.

However, some personal information collected through the FOTM project may be disclosed to internal CBSA stakeholders, such as IED, if a rover officer is not able to intercept an individual before the individual leaves the airport. This will only include the information provided to the roving officer, including the traveller’s name, FOSS ID, warnings, and possibly a scene photograph.

It is noted that if any PDD individuals are identified during the short-term project, they are immediately deported without any judicial review. As the PDD is comprised of individuals who have been deported and have re-entered Canada at least one time after the initial deportation, judicial review is not available to them. Therefore, if any individual on the PDD is identified by the project, there is no sharing of the project data to the Department of Justice (DOJ), Public Prosecution Service of Canada (PPSC), Immigration and Refugee Board (IRB), or any other organization. Sharing of information on individuals who are identified by the project but are not intercepted before leaving the airport, would be limited to disclosure to IED, who would utilize the information as any other tip and use existing procedures and CBSA systems (not the FOTM FR system) to validate the status of the individual as a Previously Deported Person and attempt to locate him/her.

Risk: *There is a risk that FR matches may be inappropriately used to support further investigation by the CBSA, which could later lead to proceedings under the Immigration and Refugee Protection Act, related regulations, or under the Criminal Code before the CBSA has had an opportunity to test the efficacy of the solution.*

Mitigation: *The CBSA will ensure that appropriate procedures are in place to support a match that is referred to CBSA investigators with the caveat that the accuracy of this information cannot be verified. Specifically, before such a disclosure occurs, significant human intervention will properly assess the data match and ramifications of using FOTM FR match in a deportation proceeding. Also, once the secondary BSO is notified of a match by the Rover BSO, existing identity validation procedures are taken before the individual is deported.*

Also, if an individual departs Pearson Airport prior to being intercepted, information on the individual may be shared with Inland Enforcement. In turn, Inland Enforcement will ensure that identification steps are taken before any deportation proceedings are initiated.

Risk: *There is a risk that project handheld devices may be viewable by individuals in the CBSA-controlled area of Terminal 3. Moreover, there is a risk that BSOs will inadvertently release personal information of PDD individuals to those individuals who were falsely identified by the FR system.*

Mitigation: *The CBSA will develop procedures to ensure that, when questioning a traveller who has been selected for secondary examination on the basis of FOTM, the traveller will not be told the name of the person on the PDD against whom the traveller has been matched. The traveller will not be shown the photograph of the person on the PDD. This will ensure that falsely matched travellers are not*

inadvertently given information about persons of interest. These same procedures, and related training, will instill in Rover BSOs the need to shield the handheld screen when in on the floor.

Risk: *The Standard Operating Procedures designed to support the activities of the CBSA staff at Terminal 3 have not yet been finalized and approved. These procedures will:*

- *support an expedited identity of travellers to determine if secondary examination is necessary;*
- *For false positives, require a quick release process;*
- *Ensure handheld device screens are shielded from view by individuals on the floor;*
- *Restrict disclosure of PDD data and the photograph; i.e. individuals who are interviewed by the Rover BSO and at secondary will not be shown PDD data/photos;*

Mitigation: *The CBSA should refrain from initiating the demonstration project until the procedures have been approved, communicated to staff, and appropriate training has been provided.*

ACCURACY

Within the CBSA

Throughout the PIA process, the ATIP Division works with program areas to ensure that CBSA programs create a process for ensuring the accuracy of information as required, and that program areas are capable of handling requests for correction of personal information.

The correction process is coordinated centrally from the ATIP Division. Requests for correction are forwarded to the appropriate program area for action. A response letter is sent to the client indicating whether the correction was accepted or refused, whether the correction is made directly or notated to the file, and whether or not that information has been disclosed and that those recipients would be informed appropriately. The ATIP Division is looking at developing a more standardized approach and directive for the processing of correction requests.

Specific to the Faces on the Move Project

The CBSA recognizes that the accuracy of the matching algorithm has not yet been proven; the Agency has taken measures to mitigate this privacy risk. When installing the dedicated cameras, the CBSA will carefully calibrate the environment to ensure that light levels, camera angles, and lines of sight have been optimized to ensure that high-quality images are obtained. When the FOTM project becomes operational, the CBSA has also implemented policies and procedures to ensure that all matches produced by the system are first verified by a specially trained human operator before being actioned. Finally, the CBSA will continually refine these conditions to enhance the accuracy of the project throughout its duration. However, as the goal of the project is to test the accuracy of the system, there is a significant residual privacy risk to operational FR matching which cannot be mitigated without first conducting the FOTM project.

Risk: *The FOTM project may incorrectly refer travellers for secondary examination based on a false positive match.*

Mitigation: *The CBSA has implemented a number of measures to reduce the rate of false positives by controlling environmental factors, ensuring human verification, and verifying the accuracy of a match during the secondary examination process.*

Recommendation: *The CBSA should implement a limit to the rate of false positives and consider deactivating the project if it exceeds this rate.*

SAFEGUARDS

Within the CBSA

Typically the ATIP Division strongly recommends the completion of a TRA and SoS as part of the PIA process, and directs programs to contact Corporate Security for guidance with respect to those instruments. A summary of the risks identified in a TRA are appended to the PIA to ensure that all risks are identified and mitigated by the program area.

CBSA employees are required to take the online CBSA Security Awareness course when they begin employment, and to refresh their training every two years. CBSA managers are required to take both the CBSA Security Awareness course and a CBSA Security Awareness course for managers.

The Privacy Breach Protocol complements existing CBSA security policies, and ensures that all security violations which include personal information are reported to the ATIP Division in addition to the Security and Professional Standards Division, and outlines the roles and responsibilities of the Agency with respect to privacy breaches, which may include notification of the individuals, notification of the Office of the Privacy Commissioner, and the identification of mitigating measures.

Specific to Faces on the Move Project

Although a Threat and Risk Assessment (TRA) is currently underway, the CBSA has incorporated a number of safeguards to protect personal information under its control. Personal information used in this program been rated as Protected B and will be safeguarded in accordance with the *Management of Information Technology Security* (MITS) when it is installed. This includes, but is not limited to: securing physical assets in a location with limited access, restricting user access to the system, and encrypting all data transmission to prevent compromise. Further technical and administrative safeguards are currently being evaluated through the TRA process.

Further, the initial draft of this PIA did not examine the use of cellular networks for transmitting personal information to roving BSOs. A wireless network is necessary for match alerts because the receiving CBSA officer is patrolling the airport and the conditions of the terminal do not permit a Wi-Fi network to be created for technical reasons. The scope of the PIA was expanded to include this data flow and relevant program areas within the CBSA, including Corporate Security and Information Management, were engaged to ensure that the CBSA has proper safeguards and accountability mechanisms for personal information it transmits through these networks.

Risk: *The personal information being transmitted on a wireless network may be compromised.*

Recommendation: *The CBSA will ensure that all wireless transmission of data is secure using appropriate encryption technologies. Any transmission of recordings over wireless networks must be done in accordance with the CBSA's Policy on the Use of Wireless Technologies. Wireless transmission of data not in compliance with these protocols must cease immediately and the wireless transmission can only resume when authorized by local IT and an official of the Physical Security Section of the Security and Professional Standards Directorate. A Security Assessment of FOTM, including wireless alert transmission, is underway and will be forwarded when it is complete.*

Risk: *The system has been configured to enable remote access by system administrators.*

Recommendation: *Remote access should be secure using appropriate encryption techniques.*

OPENNESS

Within the CBSA

The CBSA manages its Info Source chapter directly on the CBSA website at <http://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/pia-efvp/atip-aiprp/infosource-eng.html>. The ATIP Division ensures that the descriptions of program privacy practices are kept complete and up-to-date.

The Directive on Privacy Impact Assessments requires departments to ensure that PIA summaries in both official languages are made available to the public. At a minimum the summary must address section 1 and 2 of the Core PIA Template. CBSA PIA summaries are posted at <http://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/pia-efvp/atip-aiprp/pias-sefp-eng.html>.

Upon completion of a PIA, PIA summaries are posted on the CBSA website, which also contains information on accessing personal information at the CBSA.

Specific to Faces on the Move Project

As reflected in Section 7 of this PIA (Question 17.5), notice of camera use to support the FOTM demonstration project will not be provided in any form. The CBSA already collects Overt Audio-Video Surveillance as part of its normal port operations. Signs throughout the facility indicate that travellers are under video surveillance and direct travellers to the CBSA's website or a supervisor for more information. |

Failing to provide such notice is authorized pursuant to sub-section 5(3) of the *Privacy Act*.

In lieu of signage, the CBSA has developed a communications strategy, which includes posting an executive summary of this PIA, for communicating the general purposes of the FOTM project. The CBSA intends to proactively disseminate information about the FOTM project through a news release and a dedicated section on its corporate website. All communications materials will indicate the purposes and general function of the FOTM project but will not specify where it installed, which database it will use, or when it will be operational.

Risk: *The use of FR software is not supported by notice to individuals who enter the testing area.*

Mitigation: *The CBSA will not mitigate this risk by posting additional signage or modifying existing signage. Failure to provide notice in these circumstances is consistent with sub-section 5(3) of the Privacy Act which authorizes the CBSA to refrain from notice if, by providing such notice, may result in inaccurate information, may defeat the purpose of the collection, and/or may prejudice the use of the information collection.*

SECTION 9 - SUPPLEMENTARY DOCUMENTS LIST

Additional documents used or related to the PIA may include:

- *CBSA Policy on the Overt Use of Audio-Video Monitoring and Recording Technology*
- *CBSA Directives on the Overt Use of Audio Video Monitoring and Recording Technology*
- *CBSA PIA on the Overt Use of Video Monitoring and Recording Technology*
- *CBSA Comptrollership Manual – Security Volume Chapter 6: Storage of Sensitive Information and Assets*
- *CBSA Comptrollership Manual – Security Volume Chapter 8: Disposal of Sensitive Information and Assets*
- *CBSA Policy on the Use of Wireless Technology*
- *CBSA Guidelines for the Directive on the Use of Wireless Technology*
- *Immigration and Refugee Protection Act*
- *CBSA Policy on the Disclosure of Customs Information: Section 107 of the Customs Act (formerly D1-16-1 and D1-16-2)*
- *CBSA Policy on the Disclosure of Personal Information: Section 8 of the Privacy Act*
- *CBSA Enforcement Manual Part 7 / Chapter 3*
- *CCTV Class of Records*
- *CCTV Personal Information Bank*
- *Video Recording and Monitoring Privacy Notice*
- *Video Surveillance Signage*
- *Audio and Video Signage*
- *Video Surveillance Sign Locations*
- *Privacy Notification given at interview rooms, primary inspection areas, secondary inspection areas and cash/information counters*
- *Inventory of Cameras*
- *PIA Action Plan*
- *Security Assessment Summary (work in progress)*
- *Security Action Plan*
- *Canadian Safety and Security Program Project Charter — CSSP-2014-CP-2000*
- *OPC Report: Automated Facial Recognition In the Public and Private Sectors*
- *OPC Report: At Your Fingertips – Biometrics and the Challenges to Privacy*
- *OPC Guidance: Guidance for the Use of Body-Worn Cameras by Law Enforcement*

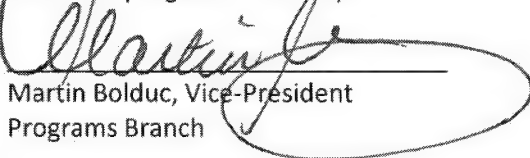
PROTECTED B

Faces on the Move: Multi-camera Watchlist Screening

PIA

SECTION 10 - FORMAL APPROVAL

The following signature represents a commitment to comply with sections 4 to 8 of the Privacy Act and the related privacy policy requirements outlined in the PIA as they relate to the administration of the identified program or activity.


Martin Bolduc, Vice-President
Programs Branch

Signature of PIA lead for program or activity

22/01/2016
Date

Note: Responsibility for sections 4 to 8 of the Privacy Act rests with all employees of government institutions that handle personal information. Officials who manage such programs and activities are responsible for ensuring that such requirements are implemented as part of the administration of the program or activity.

The following signature represents a commitment by the Head of the institution or his/her delegate(s) who is responsible for establishing personal information banks in accordance with section 10 of the Privacy Act.


Dan Proulx, Director, ATIP Division,
Corporate Affairs Branch

Signature of Head of the institution or the delegate responsible for Section 10 under the Privacy Act

22/01/2016
Date

Note: Under the Privacy Act, the Head or his/her delegate(s) is responsible for complying with legal and relevant privacy policy requirements related to the approval and registration of personal information banks



Secure and Trusted Partnerships / Trusted Traveller / NEXUS

Privacy Impact Assessment (PIA)

**Trusted Traveller Programs
Program and Policy Management Division, Programs Branch
December / 2016 / Ver. 1.3**



Canada

Version Control

Version	Author	Action	Date
1.0	Lyne Pelletier	Creation of document includes Treasury Board Secretariat policy requirements (2010). Incorporates more detailed privacy analysis to reflect expectations of the Office of the Privacy Commissioner (2011). User friendly with examples and explanatory notes. Includes an Action Plan for implementing mitigating strategies.	March 15, 2012
1.0	Dan Proulx	Approved ver. 1.0	March 28, 2012
1.1	Lyne Pelletier	Oakes Test and Privacy Principles added to template	November 07, 2012
1.2	Dan Proulx	Approved ver. 1.1	November 15, 2012

Change Control Table

Version	Date	Change Made By	Change Requested By	Change
1.0	March 10, 2011	Final PIA submitted to OPC		
1.1	February 9, 2015	Adam Norwick, Greg Reiser	Rob Gilbert Adam Norwick	Update template and PIA for program changes
1.2	February 26, 2016	Nicholas Koutros Adam Norwick	Nicholas Koutros Adam Norwick	Finalized PIB text, added comments on four-part test, consistency throughout PIA
1.3	June 2016	Greg Reiser Sandra Desormeaux	ATIP, Information Sharing & Collaborative Arrangements Policy, Legal Services, Trusted Traveller Programs unit, Business Systems Integration Division, Traveller Operations Division, Alternate Reporting unit, Stakeholder Engagement & Outreach unit, Information Management and Information Technology - Security	Update PIA with program changes

Privacy Impact Assessment Template - Overview

Privacy is protected by national and international law, and for this reason, Treasury Board Secretariat (TBS) requires that any new or substantially modified program or activity involving the collection, use, disclosure or retention of personal information be assessed for privacy impacts. The Privacy Impact Assessment (PIA) is a tool used to identify risks and to describe strategies to remove or reduce these risks.

THE PIA PROCESS

The program contacts the Access to Information (ATI) and Privacy Division at the planning stage of a new initiative. **Sections 1 and 2** of this template will be used to determine whether a PIA is required, or whether the CBSA Privacy Protocol for Non-Administrative Purposes (2012) must be implemented.

When a PIA is recommended, the program appoints a drafter, normally a subject matter expert. The program meets with an ATI and Privacy advisor, and a timeline for completion of each phase of the PIA is set.

The PIA can be a complex undertaking, requiring technical input from a variety of sources such as IT Security, Legal Services, Information Management, Contracting and Procurement, and in some cases, other government departments or foreign jurisdictions. At the same time, the intended audience of the PIA is the privacy advisor with the Office of the Privacy Commissioner (OPC) of Canada, who have little knowledge of CBSA programs or systems. For this reason, the PIA must be written in plain language, understandable to a non-CBSA reader. Jargon must be avoided, and acronyms should be spelled out.

When completed, the ATI and Privacy Director and the Vice President lead for the program or activity endorses the final PIA, which is then transmitted by the ATI and Privacy Division to the Office of the Privacy Commissioner for their review and to Treasury Board Secretariat for the registration of new or modified Personal Information Banks (PIB). An executive summary is then posted on the **CBSA website**.

Please note that all text in blue, the various notes, examples, and statutory and policy references provided throughout the template are included as guidance to help the drafter complete the PIA template. These references must be deleted as the PIA is being completed.

Table of Contents

VERSION CONTROL.....	2
PRIVACY IMPACT ASSESSMENT TEMPLATE - OVERVIEW	4
EXECUTIVE SUMMARY	7
ABBREVIATIONS AND ACRONYMS	11
DEFINITIONS	14
INTRODUCTION	15
Background/Overview of the Program	15
Roles and Responsibilities	21
Scope of the PIA	24
SECTION 1 - OVERVIEW AND INITIATION	25
SECTION 2 - RISK AREA IDENTIFICATION AND CATEGORIZATION	31
SECTION 3 - ANALYSIS OF PERSONAL INFORMATION ELEMENTS	38
SECTION 4 - FLOW OF PERSONAL INFORMATION	42
4.1. Information Systems	42
4.2. Audit of NEXUS Use	59
4.3. Retention of NEXUS Data	59
4.4. Data Flow Model - Table	60
4.5. Internal Use and Disclosure	61
4.6. External Use and Disclosure	61
4.7. Retention / Storage	62
4.8. Other Possible Considerations	63
SECTION 5 - PRIVACY COMPLIANCE ANALYSIS	64
1. Legal Authority For Collection Of Personal Information	64
2. Necessity To Collect Personal Information	64
3. Authority For the Collection, Use or Disclosure Of the Social Insurance Number	65
4. Direct Collection - Notification and Consent (as appropriate)	66
5. Indirect Collection - Consent or Authority Under Sec. 10 of Privacy Regulations	67
6. Indirect Collection - Without Notification and Consent	69
7. Retention and Disposal of Personal Information	70
8. Accuracy Of Personal Information	72
9. Use Of Personal Information	74

10. Disclosures Directly Related to the Administration of the Program or Activity	75
11. Accounting For New Uses or Disclosures Not Reported in CBSA Info Source	77
12. Safeguards - Statement Of Sensitivity.....	79
13. Safeguards - Threat and Risk Assessment.....	80
14. Safeguards - Administrative, Physical and Technical	81
15. Technology and Privacy - Tracking Technologies.....	83
16. Technology and Privacy - Surveillance or Monitoring.....	84
17. Considerations Related to Compliance, Regulatory Investigation, Enforcement.....	85
SECTION 6 - SUMMARY OF ANALYSIS AND RECOMMENDATIONS	86
SECTION 7 - SUPPLEMENTARY DOCUMENTS LIST.....	101
SECTION 8 - FORMAL APPROVAL	104
ANNEX A: PRIVACY COMPLIANCE CHECKLIST AND OTHER CONSIDERATIONS	105
ANNEX B: OFFICE OF THE PRIVACY COMMISSIONER EXPECTATIONS.....	108
ANNEX C: CATEGORIES OF PERSONAL INFORMATION.....	111
ANNEX D: CONTROLS AND PROCEDURES IMPLEMENTED TO LIMIT PERSONAL INFORMATION COLLECTION	113
ANNEX E: CONTROLS AND PROCEDURES IMPLEMENTED TO DOCUMENTING CONSENT AND WITHDRAWAL OF CONSENT	114
ANNEX F: CONTROLS AND PROCEDURES IMPLEMENTED FOR RETENTION AND DISPOSAL OF PERSONAL INFORMATION.....	116
ANNEX G: CONTROLS AND PROCEDURES IMPLEMENTED FOR ACCURACY OF PERSONAL INFORMATION	118
ANNEX H: CONTROLS AND PROCEDURES IMPLEMENTED TO LIMIT ACCESS TO PERSONAL INFORMATION	119

Privacy Impact Assessment Date / Version:	2011-03-10 (Originally received by OPC)
Office of the Privacy Commissioner file #:	000546
Federal Institution:	Canada Border Services Agency (CBSA)
Related Class of Record Number:	CBSA ADM 117
Personal Information Bank:	CBSA PPU 031
Government Official Responsible for PIA:	Vice President, (Programs Branch)
Delegate for section 10 of the <i>Privacy Act</i> :	ATIP Director

EXECUTIVE SUMMARY

NEXUS Privacy Impact Assessment

NEXUS is a bi-national Canada-United States (U.S.) program managed by the Canada Border Services Agency (CBSA) and U.S. Customs and Border Protection (CBP). The Traveller Programs Directorate of the Programs Branch at the CBSA is the Office of Primary Interest (OPI) for NEXUS.

NEXUS allows for customs and immigration border clearance processes to be streamlined for pre-approved, low-risk travellers, thus permitting the CBSA and CBP resources to be allocated more effectively at the border. Membership is five years and provides expedited border clearance into Canada and the U.S. in the land, air and marine travel modes. In 2002, the NEXUS program was delivered in a travel mode specific format, beginning with the NEXUS Highway Program. Subsequently in 2006, the NEXUS suite of programs was harmonized to provide members with expedited travel privileges in all three travel modes (land, air, and marine). NEXUS members use dedicated lanes in the highway mode; self-serve kiosks in the air mode; and, by reporting through Telephone Reporting Centres (TRC) in the marine mode.

To become a member of the NEXUS program, an applicant voluntarily submits an application using either a paper form sent to the CBSA or by applying electronically using the Global Online Enrollment System (GOES) maintained by CBP. When a paper application form is used, a clerk enters the information into the Global Enrolment Component (GEC) of the Integrated Customs System (ICS) and it is assessed against a variety of enforcement databases to determine program eligibility. The personal information entered by the applicant is used by the CBSA and CBP to confirm their identity and to determine the eligibility of an applicant and the continued eligibility of a member.

When an applicant is accepted as a NEXUS member, periodic risking is performed as well as *ad hoc* risking based on cause. Also, an assessment is performed at each passage to confirm if there have been any infractions that would result in the revocation of the membership or in the inadmissibility of the member into either Canada or the U.S.

On March 10, 2011, a Privacy Impact Assessment (PIA) for the NEXUS program was submitted to the Office of the Privacy Commissioner of Canada (OPC). Observations and recommendations made by the OPC in August 2011 were addressed, and communication with that office continues as the NEXUS program evolves. Since the original NEXUS PIA, the following developments have occurred that impact

the NEXUS program:

- The Canadian Air Transport Security Authority (CATSA) has implemented the Trusted Traveller CATSA Security Lines to provide dedicated CATSA security screening lines to NEXUS members at airports; it has also deployed an automated gate pilot project at the Edmonton International Airport;
- New NEXUS kiosks have been installed at tier 1 Canadian airports and Billy Bishop Toronto City International Airport;
- In 2014, the CBSA launched a pilot project called NEXUS Electronic Gate (eGate) to allow 24/7 access to the NEXUS lane at the Peace Bridge land border port of entry at Fort Erie, Ontario;
- The CBSA and CBP are seeking to expand eligibility of the program to third country nationals that are members of their own domestic program, where an arrangement between the three parties is forged; and
- Vicinity Radio Frequency Identification (RFID) allows faster secure capture of individual traveller information while in the Primary Inspection Line (PIL) prior to their arrival at the primary inspection booth; RFID technology is used for NEXUS Highway.

These developments are included in this updated NEXUS PIA that will be submitted to the OPC. Please note that the proposed CBSA-Canadian Security Intelligence Service (CSIS) pilot project that would share information with CSIS as part of the risk assessment process, is being dealt with in a separate multi-institutional PIA.

Protecting your Personal Information

The following personal information elements will be managed by the NEXUS program:

- full name
- contact information
- signature
- biographical information
- biometric information (for air travel only)
- citizenship status
- criminal checks/history
- date of birth
- credit card information (if not paying by certified cheque or money order); and
- identification numbers such as those contained on the birth certificate, driver's license or passport.

Personal information is not disclosed to other federal departments during the risk assessment process. Rather, the CBSA uses the information to run queries in other institution's databases, which the CBSA has access to:

- **CPIC – "Canadian Police Information Centre" (Royal Canadian Mounted Police)** - Contains wants/warrants and criminal records.
- **NCIC – "National Crime Information Center of the United States"** – Contains U.S. national intelligence information – wants/warrants and criminal records.

- **IBAS – “Interdiction and Border Alert System” (Immigration, Refugees and Citizenship Canada)**
 - Searchable for Criminal Removals; Lost, Stolen, Fraudulent documents (LSFDs) which includes passport data from Passport Canada; TUSCAN lookouts (Tipoff US Canada); IRCC issued documents (valid documents); Immigration Enforcement Indicators (IEIs)

The “**Integrated Customs Enforcement System**” (ICES) is a CBSA database that contains customs seizures for a period of six years plus the current year, and current data. The ICES also contains customs/immigration lookouts.

The pass/fail result of the risk assessment both at initial enrolment and during periodic risk assessment is shared with CBP as part of the eligibility and continued eligibility determination process. Pursuant to s. 107 of the *Customs Act*, information regarding admissibility may be disclosed to IRCC and within the CBSA to enforce the *Immigration and Refugee Protection Act* and the *Customs Act* respectively, and information may be shared with accredited domestic law enforcement agencies engaged in the administration or enforcement of the law, and in the detection, prevention, or suppression of a crime. CBP conducts its own risk assessment process against its respective domestic law enforcement, immigration, customs, and criminal and intelligence databases to determine the applicant’s eligibility and continued eligibility into the NEXUS program. CBP shares only the pass/fail result with the CBSA. For both the CBSA and CBP, the reason for rejection of an application or cancellation of a membership is not shared between the two agencies.

The collection of information for the NEXUS program is used to determine an applicant’s eligibility for inclusion in the program, as well as his/her ongoing eligibility.

Right of Access

A Privacy Notice statement appears on the paper application form and is also presented on the GOES screen when applying on-line. The Privacy Notice statement describes the purpose, use, disclosure and retention of personal information collected or created as part of the NEXUS program.

Pursuant to the *Privacy Act* and its regulations, the *Canada Evidence Act* and the *Customs Act*, the retention periods for NEXUS information are as follows:

Electronic and paper applications may be destroyed according to the following schedule:

- **Rejected applications for NEXUS:** The application forms and accompanying documents may be destroyed two years after the redress period has expired if there has been no request for redress. This information is kept in order to satisfy *Privacy Act* requirements to keep personal information for two years following the last administrative use, and to allow refused applicants the opportunity for redress.
- **Successful applicants for NEXUS:** The applications may be destroyed six years after the date on which an application is approved. The retention period for the accompanying documents is two years following the last time the personal information was used for an administrative purpose.
- **Where the Canadian Processing Centre (CPC) is scanning and creating electronic records of application forms,** the paper applications may be destroyed once electronic copies have been

made. The electronic copies should be retained according to the same paper application retention schedule above.

Biometric information may be destroyed according to the following schedule:

- Rejected applicants to NEXUS: Failed applicants do not provide any biometric data.
- Successful applicants to NEXUS: Only approved members are required to provide a photograph and fingerprints (fingerprints are collected by CBP only and are not shared with the CBSA). Iris biometrics are an additional option for those members who wish to use self-serve kiosks in airports. The retention period for the photograph and the initial iris scan taken at the time of enrolment is at least two years. Iris templates used to identify a member at time of passage are kept for a period of two years following each passage.

You may formally request access to your personal information, or access to corporate records related to or created by the NEXUS program by contacting the ATI and Privacy Division. More information about this can be found at: <http://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/pia-efvp/atip-aiprp/menu-eng.html>.

Accountability

If you have concerns about the collection, use, disclosure or retention of your personal information, you may issue a complaint to the CBSA ATI and Privacy Division. Complaints should be made in writing and include your name, contact information, and a brief description of your concerns. Contact information for the ATI and Privacy Division at the CBSA can be found **here**.

If you are denied or revoked from the NEXUS program by CBP, you will be provided the process for seeking clarification in writing. You may also challenge the decision by contacting the local trusted traveller Enrolment Centre or by writing to the CBP Trusted Traveller Ombudsman. Further information on these processes can be found at <http://www.cbp.gov/travel/trusted-traveler-programs/program-denials>.

If you are denied membership in the NEXUS program or are cancelled or suspended from the program by the CBSA, you may write to the Recourse Directorate at Headquarters or on-line to request a review of the decision within 90 days of the date shown on the NEXUS letter. Further information on these processes can be found at <http://www.cbsa-asfc.gc.ca/prog/nexus/term-eng.html>.

ABBREVIATIONS AND ACRONYMS

The following is a list of abbreviations and acronyms used in this report:

ATIA	<i>Access to Information Act</i>
ATIP	Access to Information and Privacy
BUC	Business Use Case
BSO	Border Services Officer
CA	<i>Customs Act</i>
CATSA	Canadian Air Transport Security Authority
CBSA	Canada Border Services Agency
CEA	<i>Canada Evidence Act</i>
CLF	Common Look and Feel
CoR	Class of Record
CPC	Canadian Processing Centre
CPCS	Canadian Processing Centre System
CPIC	Canadian Police Information Centre
CRA	Canada Revenue Agency
DOB	Date of Birth
DSO	Departmental Security Officer
EC	Enrolment Centre
eGate	Electronic Gate
GCMS	Global Case Management System
GE	Global Entry
GEC	Global Enrolment Component
GoC	Government of Canada
GES	Global Enrolment System (U.S.)
GOES	Global Online Enrolment System (U.S.)
HQ	Headquarters
IBAS	Interdiction and Border Alert Systems
ICES	Integrated Customs Enforcement System

ICS	Integrated Customs System
ID	Identification
IQS	Integrated Query System
INM	Instituto Nacional de Migracion (Mexico)
IRCC	Immigration, Refugees and Citizenship Canada
IRPA	<i>Immigration and Refugee Protection Act</i>
ISA	Information Sharing Agreement
IT/IM	Information Technology/Information Management
LACA	<i>Library and Archives Canada Act</i>
LAN	Local Area Network
MITS	Management of Information Technology
MoU	Memorandum of Understanding
NCIC	National Crime Information Centre System (U.S.)
LAC	Library and Archives Canada
OPC	Office of the Privacy Commissioner of Canada
PA	<i>Privacy Act</i>
PCMLTFA	<i>Proceeds of Crime (Money Laundering) and Terrorists and Financing Act</i>
PDF	Portable Document Format
PGS	Policy on Government Security
PI	Personal Information
PIA	Privacy Impact Assessment
PIB	Personal Information Bank
PIL	Primary Inspection Line
PNS	Privacy Notice Standard
POE	Port of Entry
PSPC	Public Services and Procurement Canada
RAC	Risk Assessment Component
RFID	Radio Frequency Identification
RDA	Record Disposition Authority
RCMP	Royal Canadian Mounted Police
SOGD	Selected Other Government Departments

NEXUS Program

PIA

SLA	Service Level Agreement
SSC	Shared Services Canada
SOPs	Standard Operating Procedures
SoS	Statement of Sensitivity
TBS	Treasury Board Secretariat
TDC	Traveller Declaration Card
TPSD	Travellers Project and Systems Division
TRA	Threat and Risk Assessment
TRC	Telephone Reporting Centres
TRCS	Telephone Reporting Center System
TTCSL	Trusted Traveller CATSA Security Line
TTP	Trusted Traveller Programs
URL	Uniform Resource Locator [web address]
U.S. CBP	United States Customs and Border Protection
U.S. DHS	United States Department of Homeland Security
U.S. GPO	United States Government Printing Office
VP	Vice-President
VPN	Virtual Private Network
WAN	Wide Area Network

DEFINITIONS

This section provides definitions of the terms frequently used in this report:

Action Plan	The Action Plan describes the steps that the Program will take to address risks that have been identified by ATI and Privacy Division, OPC and TBS.
Administrative purpose	The <i>Privacy Act</i> defines an "administrative purpose" to be the use of an individual's personal information in a decision-making process that directly affects that individual.
Confidentiality	The Government Security Policy (2002) defines "confidentiality" to be the attribute that information must not be disclosed to unauthorized individuals, because of the resulting injury to national or other interests, with reference to specific provisions of the <i>Access to Information Act</i> and the <i>Privacy Act</i> .
Consistent use	Is a use that has a reasonable and direct connection to the original purpose(s) for which the information was obtained or compiled. This means that the original purpose and the proposed purpose are so closely related that the individual would expect that the information would be used for the consistent purpose, even if the use is not spelled out.
Data Matching	A comparison of personal data obtained from a variety of sources, including personal information banks, for the purpose of making decisions about the individuals to whom the data pertains. Data matching is a specialized activity involving the collection, use and disclosure of personal information that is subject to the various requirements of the <i>Privacy Act</i> .
Info Source	Is a series of annual Treasury Board Secretariat (TBS) publications in which government institutions are required to describe their institutions, program responsibilities and information holdings, including PIBs and classes of personal information. The descriptions are to contain sufficient clarity and detail to facilitate the exercise of the right of access under the <i>Privacy Act</i> . Data-matching activities, use of the SIN and all activities for which privacy impact assessments were conducted have to be cited in <i>Info Source</i> PIBs, as applicable. The <i>Info Source</i> publications also provide contact information for government institutions as well as summaries of court cases and statistics on access requests.
Personal Information	Personal Information: Information about an identifiable individual as defined in section 3 of the <i>Privacy Act</i> . This definition, although lengthy, is not exhaustive, as indicated by the introductory phrase, "including, without restricting the generality of the foregoing". Information that is not specifically mentioned in the list may still be included in the definition of personal information if it qualifies as "information about an identifiable individual".
Personal Information Bank	Is a description of personal information that is organized and retrievable by a person's name or by an identifying number, symbol or other particular assigned only to that person. The personal information described in the personal information bank has been used, is being used, or is available for an administrative purpose and is under the control of a government institution.
Privacy	The Office of the Privacy Commissioner describes "privacy" as "... the right to control access to one's person and information about one's self. The right to privacy means that individuals get to decide what and how much information to give up, to whom it is given, and for what uses."

INTRODUCTION

Background/Overview of the Program

The NEXUS program offers travellers a means to present themselves in an alternative manner upon arrival in Canada because they have been determined to be of low-risk based on pre-screening against criminal, immigration and customs databases. This program allows the CBSA to focus its limited resources on persons of high or unknown risk while facilitating the entry of persons who are authorized by the Minister of Public Safety.

CBSA is responsible for controlling the movement of persons and goods into Canada. By offering the bi-national NEXUS program (with the U.S.), the contributing partners determine who qualifies to be a low-risk, pre-approved member for border crossing purposes.

Through NEXUS, travellers enjoy expedited clearance into Canada and the U.S. by using dedicated lanes in the highway mode; self-serve kiosks in the air mode; and, by reporting through Telephone Reporting Centres (TRC) in the marine mode. This also benefits non-NEXUS travellers by reducing line-ups in the regular PIL.

Personal information data collected by the CBSA for the NEXUS program is used to make a determination on the applicant for membership eligibility and continued eligibility in the program.

Biometric information captured during enrolment (e.g. iris scan), is used to identify the member at a NEXUS kiosk upon return to Canada in the air mode. Individuals are not required to provide their iris biometric if they do not intend to travel by air.

Fingerprints are only collected by the U.S. CBP to verify the identity of the member at a Global Entry kiosk when entering the U.S. and during renewal or re-enrolment. They are not shared with the CBSA.

Personal information is collected from the application form as completed by the applicant, and with the consent of the applicant. The personal information is used by both Canada and the U.S. to determine eligibility in the NEXUS program. Only a "Pass" / "Fail" indicator is exchanged between the two countries; if one of the countries fails an applicant, the reason is not shared with the other country and membership in NEXUS is denied.

The NEXUS program is registered in the Index of PIB on Info Source under PIB #CBSA PPU 031 (see Schedule B). As of September 30, 2016, there were 1,444,374 NEXUS members.

The NEXUS PIA was originally submitted to the OPC in early 2011. The CBSA committed to providing the OPC with an update to the NEXUS PIA, when warranted. Since the PIA was originally submitted, a number of changes that affect NEXUS have occurred. Those changes are explained below:

1. **Trusted Traveller CATSA Security Lines (TTCSL):** In the Spring 2010, the CBSA supported and worked closely with the CATSA on the implementation of the TTCSL at CATSA Pre-Board Screening checkpoints which provides dedicated CATSA security screening lines to NEXUS members at the eight major airports as well as select medium-sized airports in Canada. Visual card verification by a CATSA screening officer is performed.

A pilot ran from March 2013 until December 2013, at the Vancouver International Airport whereby the CBSA was responsible for in-house system changes to allow CATSA to ping the GEC database, which houses NEXUS membership data. Machine-readable zone technology (the swiping of the black strip on the back of the NEXUS card) was used at the beginning of the pilot but by the end, RFID technology had been implemented. Only RFID technology was being used when a second pilot was implemented in February 2015, at the Edmonton International Airport (the automated gate solution continues to be used at this airport). The CBSA and CATSA use RFID technology when a NEXUS member uses the dedicated CATSA line: the RFID embedded in the card will prompt a picture of the member associated with that card on a screen for the screening officer to view and match the person using the CATSA line. If the screening officer deems it to be a match, the officer allows the member through the gate; if it is not a match, the person is sent to the regular security screening line. Nothing more than the person's photo is displayed to the security officer in order to identify the NEXUS member at the CATSA line. After the photo is viewed by the screening officer, the CATSA information system permanently deletes the photograph. CATSA is planning to roll out an automated gate solution with RFID functionality at the new Calgary International Airport terminal in April 2017.

A Memorandum of Understanding (MoU) for the disclosure of NEXUS biometrics to CATSA to enable CATSA to develop and maintain an automated gate solution with the CBSA has been developed and is attached at Schedule UU. A Service Level Agreement (SLA) that expires on December 31, 2016, has also been signed between the CBSA and CATSA (the SLA is attached at Schedule WW). The CBSA and CATSA intend to renew both documents.

2. **Trilateral Trusted Traveller Arrangement:** Expanding NEXUS benefits beyond Canada and the U.S. is a commitment under the *Beyond the Border Action Plan* that was released by Prime Minister Harper and President Obama on December 7, 2011. The Trilateral Trusted Traveller Arrangement is based on extending eligibility criteria of the NEXUS program to third country citizens/nationals who are members of their own domestic trusted traveller program; in turn, NEXUS members would apply directly to the third country program to receive reciprocal benefits from that country. Eligible third country applicants will complete the NEXUS application form on a voluntary basis, fulfill the screening criteria, and pay the applicable fee. While the logistics around the interview process is still under discussion, the requirement for an interview remains unchanged to complete the application process.

The revocation or suspension of membership to the domestic program will be communicated for the purposes of maintenance of membership. The reasons for cancellation or suspension, however, will not be shared.

As per the North American Leaders Summit, the first Trilateral Trusted Traveller Arrangement will be with Mexico. An MoU between the CBSA, the U.S. CBP, and Mexico's Instituto Nacional de

Migracion (INM) has been developed regarding an Arrangement that includes, but is not limited to, expanding eligibility of the NEXUS program to individuals who are members of their own domestic program.

The MoU was signed at the Minister/Secretary level by all three countries on July 2015, and is attached at Schedule NN. An Operational Program Plan was approved in June 2016, which details the procedures articulated in the MoU, including those pertaining to information sharing. The program is expected to be implemented in 2017 (Schedule OO).

It is important to note that no personal information is shared between the CBSA and INM since the third party applicant applies directly through GOES who then sends the applicant's information to the CBSA for a NEXUS risk assessment. Similarly, a Canadian NEXUS member would apply directly to the third country's domestic program.

The CBSA has also entered into negotiations on a Trusted Traveller Arrangement with the United Kingdom (UK) based on extending eligibility of the NEXUS program to UK citizens that are approved members of their own *Register to Apply* program. As previously outlined in the Mexico Arrangement, the same processes to confirm membership status apply to the UK. Canadian citizens are already eligible to apply to the UK's Registered Traveller program, so there are no additional reciprocal benefits for NEXUS members and therefore no information sharing for Canadians applying to the UK program.

3. **NEXUS eGate:** In 2014, the CBSA launched the NEXUS eGate pilot at the Peace Bridge port of entry at Fort Erie, Ontario, following a request from the Niagara River Bi-national Mayors Coalition to increase NEXUS benefits, specifically with respect to expansion of hours of operation of the NEXUS lanes in the Niagara Region. The pilot consisted of two electronic gates (entrance and exit) installed in the NEXUS lane, a sensor to read the NEXUS card, video surveillance equipment to transmit images to the office and an intercom for the CBSA Border Services Officer (BSO) to communicate with members in the vehicle. While the pilot ended in May 2015, NEXUS eGate remains operational at the POE pending the results of the analysis and a decision by the Agency for a way forward with proof of concept (for details on how NEXUS eGate works, please see Schedule GG - Peace Bridge NEXUS eGate Standard Operating Procedures and Schedule HH – Peace Bridge NEXUS eGate Mock-up Drawing). The NEXUS website provides a brief description of NEXUS eGate at <http://www.cbsa-asfc.gc.ca/prog/nexus/egate-portelec-eng.html>

A BSO has the ability to access the GEC and view the NEXUS membership information and photo from within the CBSA office (using existing NEXUS technology). The capturing and storing of video transmissions is the only aspect that is new to the NEXUS program. Video of the vehicle, driver and occupants in the NEXUS lane is captured, stored and disposed of as per current CBSA Policy on the Overt Use of Audio-Video Monitoring and Recording Technology, dated November 2013. Recordings of any audio-video monitoring activity will be retained for thirty days following the date of their creation.

IT – Security, in collaboration with the Alternate Reporting unit (Office of Primary Interest for the NEXUS eGate pilot) have determined that no Statement of Sensitivity is required at this time since no additional information is being collected that is different from the current NEXUS process flow and transmission of information is in line with the current policy in place. The NEXUS eGate process flow is included at Schedule MM.

The NEXUS eGate Business Requirements for Proof of Concept at Peace Bridge, Fort Erie, is also attached at Schedule JJ.

4. **NEXUS Kiosk Replacement:** When the original NEXUS PIA was submitted to the OPC in 2011, the NEXUS kiosks were determined to be a privacy risk since they were “at the end of their life cycle that could result in critical equipment failure and could jeopardize the delivery of the NEXUS program”. This risk has now been mitigated with the installation of 86 new NEXUS kiosks that have been installed at tier 1 Canadian airports and Billy Bishop Toronto City Airport under the Kiosk Replacement Project. Please see section 6 – Summary of Analysis and Recommendations for further information on this “risk” (for the kiosk Business Use Case, the Technology Architecture Design, and TRA and SOS, see Schedules PP, QQ, and RR respectively.
5. **Vicinity Radio Frequency Identification (RFID):** Under the *Beyond the Border Action Plan*, Canada committed to implementing Radio Frequency Identification (RFID) technology in a minimum of two lanes at 11 land POEs (for a total of 22 lanes) to facilitate and expedite the secure passage of people and goods across the shared Canada-U.S. border.

The RFID initiative:

- Allows faster secure capture of individual traveller information while in PIL, prior to their arrival at the primary inspection booth;
- Allows effective risk assessment through automated queries, reducing the administrative burden on BSOs and allowing them more dedicated attention to traveller interviews where warranted; and,
- Increases public awareness of RFID-enabled documents and availability of RFID technology at Canada’s border to facilitate and expedite border-crossing

In preparation for RFID reader installation, an information technology update was made to the Integrated Primary Inspection Line (IPIL) Highway traveller processing application in October 2014 to lay the foundation, allowing NEXUS cards to be read by existing RFID-readers in flex lanes, once installed. An information technology update was made to the IPIL Highway traveller processing application on February 11, 2016 to be able to display information obtained through the new RFID readers.

Part 1: Is the new or changing program/activity necessary to meet a specific need?**Trilateral Trusted Traveller Arrangement**

The trilateral trusted traveller arrangement with the U.S. and Mexico is necessary to align with the commitments made in the *Beyond the Border Action Plan* and the 2014 North American Leaders Summit. The country selection and mandatory criteria were set out in the approved Memorandum to Cabinet in November 2013.

NEXUS eGate:

It was determined that the use of NEXUS eGate would provide NEXUS members extended access to the NEXUS lane after hours of operation at the Port of Entry (POE), without increasing risk, and providing flexibility in terms of resource management by giving BSOs the ability to perform other duties inside the office, while awaiting NEXUS traffic. A NEXUS eGate lane is operated remotely from inside the CBSA office at the Peace Bridge POE.

Trusted Traveller CATSA Security Line (TTCSL):

TTCSL provides dedicated CATSA security screening lines to NEXUS members at busy airports. The TTCSL allows NEXUS members to present themselves at a CATSA screening checkpoint to access the designated TTCSL. The need is for a procedure that continues to maintain the necessary security standards while offering NEXUS members an added benefit.

NEXUS Kiosk Replacement

When the original NEXUS PIA was submitted to the OPC in 2011, the NEXUS kiosks were determined to be a privacy risk since they were "at the end of their life cycle that could result in critical equipment failure and could jeopardize the delivery of the NEXUS program". This risk has now been mitigated with the installation of 86 new NEXUS kiosks that have been installed at tier 1 Canadian airports and Billy Bishop Toronto City Airport under the Kiosk Replacement Project.

Radio Frequency Identification (RFID):

The vicinity RFID improves the functionality of the NEXUS card in the land mode at NEXUS crossings by allowing an RFID chip to be read within three to four metres of an RFID antenna. This permits time savings as an added benefit for the NEXUS member.

Part 2: Will the new/modified collection be effective in meeting the need?**Trilateral Trusted Traveller Arrangement**

The new collection of information is only related to membership validation for third country nationals. For example, for NEXUS membership, the U.S. system will confirm that a Mexican national is a member of their own domestic program in order to satisfy the eligibility criteria as set out in Canada's regulation and policy criteria. The collection of personal information from Mexican nationals will be collected by U.S. CBP through GOES; once GOES confirms that the applicant is a member of Viajero Confiable, the applicant will only then be able to proceed with the NEXUS application. As per standard protocol, the U.S. CBP will forward the applicant's personal information to the CBSA for Canada to commence their NEXUS risk assessment. If a Mexican national is no longer a member of their own program, U.S. CBP will be notified and they will cancel their NEXUS membership. Apart from the sharing of personal

information between the U.S. CBP and Mexico's INM, in order to confirm membership in one's own program, all other information sharing is conducted as per the regular NEXUS protocol.

Conversely, for the Viajero Confiable membership, Mexico's system will confirm with the U.S. system that Canadian and U.S. applicants are NEXUS members.

The same procedure would apply for UK citizens applying to NEXUS who are already members of their domestic program, *Register to Apply*.

NEXUS eGate:

The collection of personal information remains the same as with the NEXUS program; the NEXUS eGate technology allows for a BSO to process travellers remotely from inside the POE, thereby allowing the NEXUS lane to be open for extended hours at a land border crossing. The implementation of NEXUS eGate provides flexibility to have the NEXUS lane staffed during peak hours, and then run remotely from the CBSA office at the POE during off peak hours. When being run from the office, the interaction with the NEXUS traveller occurs via an audio/visual system and the BSO raises the gate remotely once a release or refer decision is made. This allows the BSO to perform other tasks since he/she does not have to physically be at the NEXUS lane.

Trusted Traveller CATSA Security Line (TTCSL):

The modified method of security screening will continue to allow the CBSA to confirm NEXUS membership and allow for an improved passenger experience and passenger flow through the automated gate solution.

NEXUS Kiosk Replacement:

The collection of personal information remains the same but less kiosk outages are anticipated since new NEXUS kiosks have been instituted at various major airports across Canada. This will enhance the trusted traveller experience.

RFID:

This functionality will maximize the use of RFID technology, thus enhancing effectiveness of the technology.

Part 3: Is the loss of privacy proportional to the need?

NEXUS eGate/ Trusted Traveller CATSA Security Line (TTCSL)/NEXUS Kiosk Replacement/RFID:

There is no loss of privacy with the addition of these changes that affect NEXUS.

Trilateral Trusted Traveller Arrangement

There is no loss of privacy in the Arrangement as a NEXUS member who wishes to voluntarily apply to Viajero Confiable, would do so directly with that program. Similarly, a Mexican or UK applicant could voluntarily apply to NEXUS and go through the same risk assessment as a Canadian or American applicant.

Part 4: Is there a less privacy-invasive way of achieving the same end?

NEXUS is a voluntary program that expedites the border clearance process for low-risk, pre-approved travellers into Canada and the U.S. All of the new projects listed in this PIA that affect NEXUS have been initiated to either improve efficiencies or the integrity of the program. The least privacy-invasive way of achieving these efficiencies and procedures was contemplated for each change. Further, the revised Canadian Privacy and Consent Statements explain why and how an applicant's personal information is collected, used and shared. The applicant must consent to these Statements before submitting their NEXUS application.

Personal information submitted voluntarily by an applicant is required for the CBSA to perform initial and continued risk assessments to ensure an applicant is low-risk pursuant to the meaning and spirit of the NEXUS program for the duration of their membership. None of the new projects detailed in this revised PIA ask the applicant to provide any additional personal information than was required under the original PIA submitted in 2011.

Roles and Responsibilities

1. Clients

Canadians, Americans and Mexicans who wish to become members of the Trilateral Trusted Traveller Arrangement will first be required to become a member of their own domestic trusted traveller program (for Canada and the U.S., NEXUS would be used). Only those Canadian and U.S. citizens as well as permanent residents who have applied for an authorization to present themselves for customs and immigration inspection in an alternative manner, are eligible to apply for NEXUS membership. Canadian applicants apply either by paper application in Canada or electronically through the GOES U.S. portal.

Mexican applicants will also be required to go through the risk assessment process to become a NEXUS member. Again, each country will risk assess an applicant individually and only share their "Pass" / "Fail" indicator.

A detailed description of the data flow for Canadian applicants is provided in Section 4 of this PIA.

2. U.S. CBP

The CBSA partners with U.S. CBP to deliver NEXUS and have a shared role in setting program policy and managing the delivery of the program in their respective countries. As reflected in Section 4 of this PIA, a Canadian applicant to the NEXUS program is presented with a Privacy Notice Statement and explanatory text providing appropriate openness and clarity regarding the involvement of the U.S. CBP. Both countries perform security assessments on NEXUS applicants and share a "Pass" / "Fail" indicator. Only when both countries have provided a "Pass" is the application approved for membership in NEXUS.

An MOU has been signed between the CBSA and the U.S. CBP (see Schedule A), which, in part, provides restrictions on the use and secondary disclosures of NEXUS applicant data.

Under the Trilateral Trusted Traveller Arrangement, a Mexican national who wishes to become a NEXUS member will apply through GOES. The U.S. CBP will need to validate the applicant's identity and determine membership in the applicant's own domestic program (in this case Viajero Confiable).

Once the U.S. confirms with INM that the applicant is a member of their own domestic program, the Mexican national would then be able to proceed with the NEXUS application. The application and risk assessment process is then the same as for a Canadian or American applicant.

The CBSA and U.S. CBP independently determine an applicant's status and only share the "Pass" / "Fail" indicator.

3. Mexico's Instituto Nacional de Migracion

A Canadian citizen who is a NEXUS member and who wishes to apply to Mexico's Viajero Confiable will apply directly to that program. Mexico's INM will submit the personal information mentioned in section 2 above to the U.S. system for validation that the applicant is a NEXUS member; once done, they will risk assess the applicant according to their own domestic procedures.

It is important to note that no personal information will be shared between the CBSA and INM since a Canadian applicant to Viajero Confiable would apply directly to that program.

4. United Kingdom

The CBSA has also entered into negotiations on a Trusted Traveller Arrangement with the UK based on extending eligibility of the NEXUS program to UK citizens who are approved members of their own *Register to Apply* program. Canadian citizens are already eligible to apply to the UK's Registered Traveller program, so there are no additional reciprocal benefits for NEXUS members and therefore no information sharing for Canadians applying to the UK program.

5. Canada Revenue Agency

The Canada Revenue Agency (CRA) is responsible for user endpoint (e.g. desktop, laptop, handheld) provisioning and support services.

6. IBM Canada and Perceptics LLP

To support the devices, kiosks, and technology of the NEXUS program, the CBSA utilizes private sector contractors; however, contractors are never requested to collect, use, disclose, or retain information on behalf of the CBSA NEXUS program. Furthermore, under no circumstances do these contractors have access to personal information about NEXUS members.

IBM Canada is responsible for maintaining iris technology, kiosks and cameras for NEXUS air mode, and Perceptics LLP (Perceptics) is responsible for maintaining the highway mode lane technology and equipment (e.g. RFID). Note that for NEXUS eGate, although an RFID reader is used, it is not the same RFID reader purchased under the NEXUS Perceptics contract. It is an independently purchased reader that is specifically calibrated to only read NEXUS cards. Its sole

purpose is to open the pre-PIL gate and allow entry into the NEXUS lane. At this point, no personal information is read, stored or transmitted in any way.

In the case of IBM Canada, all support work is done on-site as required and requested by CBSA Officials. Contractors performing work on behalf of IBM Canada provide kiosk and iris camera technical services or functional improvements. There is no information stored on the kiosks, therefore, IBM contractors do not have access to the CBSA's NEXUS iris database.

Perceptics provides the CBSA with Return to Depot, Next Day Replacement, and Maintenance and Support services for the NEXUS Highway integration solution; Perceptics is not a service provider for the NEXUS kiosks or NEXUS marine. The integrated solution is comprised of vicinity card readers, license plate readers, license plate set-up, site preparation, site installation and implementation, integration software, and related support and maintenance. Perceptics contractors do not have access to personal information, including the NEXUS iris database. The hardware devices, which Perceptics maintains, do not contain any personal information.

Although neither contractor has access to personal information, the contract has been awarded in accordance with an approved Security Requirements Checklist (SRCL) and related security and privacy clauses. IBM and Perceptics contractor personnel who require access to protected information, assets or sensitive work site(s) must hold a valid Reliability screening granted by the CRA through Public Service and Procurement Canada (PSPC). Furthermore, IBM and Perceptics must not remove any protected information or assets from the identified work sites and the Contractor must ensure that its personnel are made aware of and comply with the restriction. IBM and Perceptics must also comply with the provisions of the SRCL and the Security Requirements for Protection of Sensitive Information issued by PSPCC's Canadian Industrial Security Directorate (CISD).

Additionally, the contracts with IBM and Perceptics (and any other future contractors) include the following statement regarding personal information:

Handling of Personal Information

The Contractor acknowledges that Canada is bound by the Privacy Act, R.S.C. 1985, c P-21 with respect to the protection of personal information as defined in that Act. The Contractor shall keep private and confidential any such personal information collected, created, or handled by the Contractor under the Contract, and shall not use, copy, disclose, dispose of or destroy such personal information except in accordance with this clause and the delivery provisions of the Contract. All such personal information is the property of Canada, and the Contractor shall have no right in or to that information. The Contractor shall deliver to Canada all such personal information in whatever form, including all working papers, notes, memoranda, reports, data in machine-readable format or otherwise, and documentation which have been made or obtained in relation to this Contract, upon the completion or termination of the Contract, or at such earlier time as the Minister may request. Upon delivery of the personal information to Canada, the Contractor shall have no right to retrain that information in any form and shall ensure that no record of the personal information remains in the Contractor's possession.

7. Shared Services Canada (SSC)

SSC is responsible for application and database hosting infrastructure and network services.

Scope of the PIA

The NEXUS PIA was originally submitted to the OPC in early 2011. This updated version includes descriptions of the changes that have occurred since that time that affect NEXUS i.e. Trusted Traveller CATSA Security Lines; Trilateral Trusted Traveller Arrangement; NEXUS eGate; NEXUS kiosk replacement; and, Vicinity RFID.

This assessment also includes all activities related to the collection, storage and use of personal information by the CBSA where it concerns NEXUS. It also describes what type of personal information is shared with the U.S. CBP to jointly administer the program.

The assessment does not address concerns relating to the collection, storage or use of personal information where the information is provided by the individual directly to the U.S. CBP.

SECTION 1 - OVERVIEW AND INITIATION

Report Objectives

This report is a PIA for the NEXUS program of the CBSA. The objectives of this PIA are:

- to review the business processes in order to identify the data flow of personal information;
- to analyze the collection, use, disclosure and retention of personal information;
- to determine if there are privacy risks associated with the NEXUS program; and
- to provide recommendations on the mitigation or elimination of the risks.

The information presented in this report follows the Treasury Board of Canada Secretariat Privacy Impact Assessment policy and guidelines.

The purpose of a PIA process is to ensure that privacy is considered throughout the project development cycle. The results of a PIA are a documented guarantee that privacy issues have been identified and adequately addressed.

Government Institution: Canada Border Services Agency, Programs Branch

Government Official Responsible for the
Privacy Impact Assessment

Head of the government institution / Delegate
for section 10 of the *Privacy Act*

CBSA Vice President lead for program or
activity

CBSA ATI and Privacy Director

Name of Program or Activity of the Government Institution:

Program Activity 1.2 - Secure and Trusted Partnerships \ Program Sub-Activity 1.2.1 – Trusted Traveller

Description of Program or Activity:

Secure and Trusted Partnerships

Through the Secure and Trusted Partnerships program, the CBSA works closely with clients, other government departments and international border management partners to enhance trade chain and traveller security while providing pre-approved, low-risk travellers and traders with streamlined and efficient border processes. The CBSA develops and administers programs and cooperative agreements with its partners to ensure alignment with international standards (e.g. World Customs Organization SAFE Framework of Standards) and promote best practices in global border management. By increasing membership in trusted traveller and trader programs, the CBSA is able to improve its capacity to mitigate risk in advance and focus examination efforts on identifying travellers and traders of unknown or higher risk.

Trusted Traveller

The Trusted Traveller Programs are designed to simplify the border clearance process for pre-approved, low-risk travellers entering Canada. The CBSA offers two programs for travellers, NEXUS and CANPASS. These programs

streamline (expedite and simplify) border clearance. NEXUS is a joint initiative with the U.S. CBP in the air, land and marine modes of transportation, while CANPASS is a Canadian suite of programs for clients entering Canada by plane, corporate and private aircrafts and private boats. Both programs are available to citizens or permanent residents of Canada and/or the U.S. and enable members to cross the border faster when travelling to Canada and, in the case of NEXUS, when travelling to the U.S.

Applicants to the programs must pass various assessments (e.g. security checks, interviews and risk assessments) specific to the program before being granted membership. NEXUS members can use iris recognition technology for passage processing at designated airports, and Radio Frequency Identification technology for processing at designated highway ports of entry. Members of NEXUS or the CANPASS Private Boat, CANPASS Corporate Aircraft or CANPASS Private Aircraft programs entering Canada by private aircraft, corporate aircraft or private boat must report their arrival in advance and make their declarations to the CBSA Telephone Reporting Centre.

Description of the class of records associated with the program or activity:

NEXUS Program

Description: Describes records relating to the NEXUS program. May include records related to the establishment or use of electronic systems used to administer or manage the program including the Global Online Enrollment System (GOES), the Integrated Customs System (ICS), the Integrated Customs Enforcement System (ICES), IRCC's Interdiction and Border Alert Systems (IBAS), the Royal Canadian Mounted Police's Canadian Police Information Centre (CPIC), and the U.S. Federal Bureau of Investigation's (FBI) National Crime Information Center (NCIC).

Document Types: Forms, website, program evaluation studies, member surveys, compliance reviews and investigations, Memoranda of Understanding and Information Sharing Arrangements.

Class of Record Number:

CBSA ADM 117

- ☐ Proposal for a New Personal Information Bank
- ☒ Proposal to modify an existing Personal Information Bank - identify PIB registration number and current description:

NEXUS Program Personal Information Bank

Description: This bank describes information that is about individuals who have applied to the NEXUS program. NEXUS is an expedited border clearance program jointly administered by the Canada Border Services Agency (CBSA), and the United States Customs Border Protection (CBP) with dedicated lanes at the land border, kiosks at airports and telephone reporting in marine mode for pre-approved low risk travellers. The CBSA may also enter into reciprocal arrangements with countries other than the United States that also have similar programs to extend NEXUS privileges to citizens of those countries. The personal information may include full name, contact information, biographical information, biometric information, citizenship status, credit information (credit card number), criminal checks/history, date of birth, other identification numbers, physical attributes (gender), place of birth, signature, immigration enforcement checks / history, national security assessment, pass/fail results of program eligibility checks

conducted by the CBP, and copies of travel and identification documents submitted as part of the application process.

Note: Information may be stored in the following internal systems / databases: Global Enrolment Component (GEC) of the Integrated Customs System (ICS); the Risk Assessment Component (RAC) pings the Integrated Customs Enforcement System (ICES), Interdiction Border Alert System (IBAS), Canadian Police Information Centre (CPIC), and the National Crime Information Center (NCIC) at enrolment. At each passage, ICES, IBAS and CPIC are checked. A NEXUS membership will enable air travellers to save time by using the Trusted Traveller Canadian Air Transport Security Authority (CATSA) Security Line at major and select medium-sized Canadian airports to expedite airport pre-boarding security screening.

Class of Individuals: NEXUS Program applicants.

Purpose: To determine if an applicant can be approved to participate in an expedited border clearance program. Personal information is collected pursuant to s. 11(6) of the *Customs Act* and s. 6.1 of the *Customs Act Regulations* 2003-323.

Consistent Uses: As part of the risk assessment, the Applicant's first name, middle name, last name, date of birth and gender may be used to query enforcement information from the CBSA's Integrated Customs Enforcement System (CBSA PPU 016), criminal record information from the Royal Canadian Mounted Police's Canadian Police Information Centre database (Operational Records RCMP PPU 005), and immigration enforcement information from Immigration, Refugee and Citizenship Canada's Interdiction Border Alert System (Immigration Case File CIC PPU 042)

The applicant's first name, middle name, last name, date of birth and gender may be disclosed to the U.S. Federal Bureau of Investigation to query criminal records against the National Crime Information Center database.

The member's facial photograph may be shared temporarily with CATSA to validate identity when the member uses the Trusted Traveller CATSA Security Line (Boarding Pass Security Screening PIB CATSA PPU 100).

All of the information provided directly by the applicant may be shared with the CBP in the administration of program membership, and to the U.S. Government Print Office for issuance of the NEXUS card. Only the pass/fail result from the CBSA risk assessment will be shared with the CBP to confirm an applicant's program eligibility.

Personal information may be shared within the CBSA for the following: to administer appeals concerning revocation of NEXUS membership (Enforcement and Trade Appeals CBSA PPU 005); to ports of entry to confirm valid membership for admissibility purposes in designated Trusted Traveller lanes (Traveller Processing CBSA PPU 1101); to the CBSA Enforcement and Intelligence Operations Directorate as part of the CBSA risk assessment process to check for immigration and customs infractions (CBSA PPU 018); and, to the Overt Audio-Video Surveillance area as part of the NEXUS eGate pilot at Fort Erie, Ontario (CBSA PPU 1104).

Confirmation of membership may be shared with those countries other than the United States with which the CBSA has entered into a trilateral trusted traveller arrangement that extends NEXUS privileges in accordance with those arrangements.

Retention and Disposal Standards: Applications of non-successful applicants are retained for two years following the redress period. Applications of successful applicants are retained for six years after the application is approved. Original iris scans of successful applicants are retained for at least two years, while iris scans captured at passage are kept for a period of two years. The records are then destroyed.

RDA Number: 2015/008

Related Record Number: CBSA ADM 117

TBS Registration: 002788

Bank Number: CBSA PPU 031

Legal Authority for Program or Activity:

The NEXUS program is authorized under subsection 11.1(1) of the *Customs Act* and is also governed by the *Presentation of Persons (2003) Regulations*.

Subsection 11.1(1) of the *Customs Act* states: "Subject to the regulations, the Minister may issue to any person an authorization to present himself or herself in an alternative manner."

Sections of the *Presentation of Persons (2003) Regulations* that allow for NEXUS are:

"6.1 The Minister may issue an authorization that is recognized in both Canada and the United States to a person, other than a commercial driver, to present themselves in the alternative manners described in paragraph 11(a), subparagraph 11(d)(ii) and paragraph 11(e) if the person

(a) meets the requirements set out in paragraphs 5(1)(a) to (f), subject to subsection 5(2);

(a.1) [Repealed, SOR/2015-83, s.7]

(b) has their eligibility to obtain an American authorization to present themselves on arrival in the United States in the alternative manners described in paragraph 11(a), subparagraph 11(d)(ii) and paragraph 11(e) confirmed by the United States Department of Homeland Security; and

(c) provides a copy of their fingerprints and consents in writing to their use by the Minister for the purposes of identifying the person and performing background and criminal record checks on them.

(d) [Repealed, SOR/2006-154, s.4]"

"7(1) An application for the issuance, renewal or amendment of an authorization shall be made to the Minister in the prescribed form and manner and include the applicable fee set out in section 24."

Summary of the project, initiative, or change:

Privacy is protected by national and international law, and for this reason the TBS requires that any new or substantially modified program or activity involving the collection, use, disclosure or retention of personal information be assessed for privacy impacts. The PIA is a tool used to identify risks and to describe strategies to remove or reduce these risks.

The NEXUS PIA was originally submitted to the OPC in early 2011. The CBSA committed to providing the OPC with an updated PIA when warranted. Since the PIA was originally submitted, the following changes that affect NEXUS have occurred: Trusted Traveller CATSA Security Lines; Trilateral Trusted Traveller Arrangement; NEXUS eGate; NEXUS kiosk replacement; and, Vicinity RFID update.

The NEXUS program offers travellers a means to present themselves in an alternative manner because they have been determined to be of low-risk based on pre-screening against criminal, immigration and customs databases. This program allows the CBSA to focus its limited resources on persons of high or unknown risk while facilitating the entry of persons who are authorized by the Minister of Public Safety.

Foreign governments that are involved with NEXUS include the U.S. CBP, U.S. Government Printing Office (GPO), Mexico's INM who administer their domestic trusted traveller program, Viajero Confiable (although no personal information is shared between the CBSA and INM), and the UK's Register to Apply program. Related Canadian federal government institutions include the RCMP and IRCC. Areas within CBSA include the Programs Branch, Operations Branch and the Recourse Directorate.

This PIA includes all activities relating to the collection, storage and use of personal information by the CBSA where it relates to NEXUS. It also includes the sharing of personal information with the U.S. CBP and U.S. GPO. The assessment does not address concerns relating to the collection, storage or use of personal information where the information is provided by the individual directly to the U.S. CBP.

SECTION 2 - RISK AREA IDENTIFICATION AND CATEGORIZATION

A. Type of Program or Activity

Level of Risk

Program or activity that does NOT involve a decision about an identifiable individual

☐ 1

Personal information is used strictly for statistical / research or evaluations including mailing list where no decisions are made that directly have an impact on an identifiable individual.

The Directive on PIA applies to administrative use of personal information. The Policy on Privacy Protection requires that government institutions establish an institutional Privacy Protocol for addressing non-administrative uses of personal information. *The CBSA Privacy Protocol must be implemented. Contact the ATI and Privacy Division before continuing the PIA.*

Administration of Programs / Activity and Services

☒ 2

Personal information is used to make decisions that directly affect the individual (i.e. determining eligibility for programs including authentication for accessing programs/services, administering program payments, overpayments, or support to clients, issuing or denial of permits/licenses, processing appeals, etc...).

Compliance / Regulatory investigations and enforcement

☒ 3

Personal information is used for purposes of detecting fraud or investigating possible abuses within programs where the consequences are administrative in nature (i.e. a fine, discontinuation of benefits, audit of personal income tax file or deportation in cases where national security and/or criminal enforcement is not an issue).

Criminal investigation and enforcement / National Security

☒ 4

Personal information is used for investigations and enforcement in a criminal context (i.e. decisions may lead to criminal charges/sanctions or deportation for reasons of national security or criminal enforcement).

Details: Information collected as part of the NEXUS Program is to determine an applicant's eligibility for inclusion in the program, as well as his/her ongoing eligibility.

B. Type of Personal Information Involved and Context

Level of Risk

Only personal information, with no contextual sensitivities, collected directly from the individual or provided with the consent of the individual for disclosure under an authorized program. For example: General licensing, or renewal of travel documents or identity documents.

☒ 1

Personal information, with no contextual sensitivities after the time of collection, provided by the individual with consent to also use personal information held by another source. For example: An application process with a requirement for independent verification of certain non-sensitive factual details.

☒ 2

Social Insurance Number, medical, financial or other sensitive personal information and/or the context surrounding the personal information is sensitive. Personal information of minors or incompetent individuals or involving a representative acting on behalf of the individual. For example: An individual's name on a particular list may reveal sensitive information on the health, financial situation, religious or lifestyle

☒ 3

choices of that individual.

Sensitive personal information, including detailed profiles, allegations or suspicions, bodily samples and/or the context surrounding the personal information is particularly sensitive. For example: Personal information that reveals intimate details on the health, financial situation, religious or lifestyle choices of the individual and which, by association, reveals similar details about other individuals such as relatives.

☒ 4

Details: The majority of information collected for the NEXUS program does not have any contextual sensitivity; however, to determine eligibility criminal history and checks must be performed by Canada and the U.S. The results of these checks may generate information that is particularly sensitive. However, this information will only be used to approve or reject the individual's application.

C. Program or Activity Partners and Private Sector Involvement

Level of Risk

Within the CBSA (amongst one or more programs within the CBSA)

☒ 1

With other federal institutions

☒ 2

With other or a combination of federal/ provincial and/or municipal government(s)

☐ 3

Private sector organizations or international organizations or foreign governments

☒ 4

Details: Personal information is not disclosed to other federal departments during the risk assessment process. Rather, the CBSA uses the information to run queries in other institution's databases, which the CBSA has access to. For example, IRCC's IBAS and GCMS, and the RCMP's CPIC.

Further, a trilateral trusted traveller arrangement is based on extending NEXUS eligibility criteria to third country applicants that are members of their own trusted traveller program; for example, Mexico and the UK. In these instances, a trilateral MOU is in place to allow for all three countries to exchange a positive or negative risking result, which reflects that countries' response to the applicant's inclusion in the program (Schedule NN).

D. Duration of the Program or Activity

Level of risk

One time program or activity

☐ 1

Typically involves offering a one-time support measure in the form of a grant payment as a social support mechanism.

Short-term program

☐ 2

A program or activity that supports a short-term goal with an established "sunset" date.

Long-term program

☒ 3

Existing program that has been modified or is established with no clear "sunset".

Details: The NEXUS Program is a long-term program with no sunset. The NEXUS eGate pilot in Fort Erie, Ontario ended in May 2015, but continues to function at that location. Building off the preliminary results, which suggest that the pilot had merit, the CBSA is currently finalizing a report, with recommendations for a way forward.

E. Program Population	Level of Risk
The program affects certain employees for internal administrative purposes.	<input checked="" type="checkbox"/> 1
The program affects all employees for internal administrative purposes.	<input type="checkbox"/> 2
The program affects certain individuals for external administrative purposes.	<input checked="" type="checkbox"/> 3
The program affects all individuals for external administrative purposes.	<input type="checkbox"/> 4
Details: The NEXUS Program affects only those individuals who wish to be considered for inclusion in the program. Their application is provided voluntarily with an appropriate privacy notice being provided to them. Of note, the privacy notice is clear that information will be shared with other government departments or agencies in Canada and the U.S. for the purpose of the operation of the NEXUS program (see Schedule G – NEXUS Privacy and Consent Portions of the Application Forms).	

F. Technology and Privacy	Level Of Risk
1.1 Does the new or modified program or activity involve the implementation of a new electronic system, software or application program including collaborative software (or groupware) that is implemented to support the program or activity in terms of the creation, collection or handling of personal information?	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO
<p>Details: The e-Gate technology allows the NEXUS member to provide information to the officer through an audio / visual system instead of face-to-face interaction. However, the handling of the personal information remains the same.</p> <p>With regard to RFID in the highway mode, when a traveller has scanned their NEXUS card using the RFID antenna within the lane, the IPIL Highway Application will initiate a query to retrieve traveller information, photograph, and membership status. As such, BSOs are not required to scan the same document using the document reader within the booth. NEXUS members will therefore be processed more quickly as the information will be captured for risk assessment ahead of their arrival at the PIL booth.</p> <p>The CBSA and CATSA also use RFID technology when a NEXUS member uses the dedicated CATSA line: the RFID embedded in the card will prompt a picture of the member associated with that card on a screen for the screening officer to view and match the person using the CATSA line. Nothing more than the person's photo is displayed to the security officer in order to identify the NEXUS member at the CATSA line. After the photo is viewed by the screening officer, the CATSA information system permanently deletes the photograph.</p>	
5.2. Does the new or modified program or activity require any modifications to IT legacy systems and / or services?	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO

Details: The Kiosk Replacement Plan installed 86 new NEXUS kiosks at Canadian airports to address the ageing technology and reliability issues. The new kiosks are equipped with document readers, dual printers, updated iris cameras and touch screens.

NO

6.3 Does the new or modified program or activity involve the implementation of one or more of the following technologies:

6.3.1 Enhanced identification methods:

This includes biometric technology (i.e. facial recognition, gait analysis, iris scan, fingerprint analysis, voice print, radio frequency identification (RFID), etc...) as well as easy pass technology, new identification cards including magnetic stripe cards, "smart cards" (i.e. identification cards that are embedded with either an antenna or a contact pad that is connected to a microprocessor and a memory chip or only a memory chip with non-programmable logic).

☒ YES
☐ NO

Details: An iris scan is performed at a NEXUS kiosk upon return to Canada in the air mode. The scan is not stored by the CBSA; it is only matched with the stored iris that the CBSA would have taken at NEXUS enrolment. The purpose of the iris database is for identity matching.

Vicinity RFID allows an RFID chip to be read within three to four metres of an RFID antenna in the land mode in a NEXUS lane. Once activated, the antenna reads the chip in the eligible RFID-enabled document presented by the vehicle occupants, retrieves a unique tag identifier (ID), and transmits it to CBSA systems. Chips in RFID-enabled travel documents that are not accepted under the initiative will be automatically filtered out by CBSA systems. There is no personal information contained within the RFID chip; only the unique tag ID. When the unique tag ID is received by the CBSA systems, a process is activated to send a request to the relevant secure database. It is validated and the corresponding traveller tombstone information is retrieved from the database. This information will then populate the application and a risk assessment is performed prior to presenting the biographic information and query results to the BSO.

A pilot of the TTCSL automated gate solution, using RFID technology to validate NEXUS membership, is being conducted at the domestic/international pre-board screening checkpoint at the Edmonton International Airport. When a NEXUS member uses the dedicated CATSA line, that person taps their NEXUS card at the RFID reader on the automated gate solution that will prompt a picture of the member associated with that card on a screen for a screening officer to view and match the person using the CATSA line. Nothing more than the person's photo is displayed to the screening officer in order to verify the NEXUS member at the CATSA line. After the photo is viewed by the screening officer, the CATSA information system permanently deletes the photograph.

6.3.2 Use of Surveillance:

This includes surveillance technologies such as audio/video recording devices, thermal imaging, recognition devices, RFID, surreptitious surveillance / interception, computer aided monitoring including audit trails, satellite surveillance etc.

☒ YES
☐ NO

Details: As a result of a pilot project at the Peace Bridge land border POE at Fort Erie, Ontario, called NEXUS eGate, 24/7 access is available in the NEXUS lane. While the pilot period is now over, NEXUS eGate remains functional at the POE pending the results of the analysis and a decision on a way forward. NEXUS eGate consists of two electronic gates (entrance and exit) installed in the NEXUS lane, a sensor to read the NEXUS card, video surveillance equipment to transmit images to the office and an intercom for the BSO to communicate with members in the vehicle. A BSO has the ability to access the CBSA system and view the NEXUS membership information and photo from within the CBSA office (using existing NEXUS technology). The capturing and storing of video transmission is the only aspect that is new to the NEXUS program. Video will be captured, stored and disposed of as per the Policy on the Overt Use of Audio-Video Monitoring and Recording Technology (attached at Schedule LL). There is no requirement to store audio transmissions/communications with this proof of concept.

Vicinity RFID allows an RFID chip to be read within three to four metres of an RFID antenna in the land mode in a NEXUS lane. Once activated, the antenna reads the chip in the eligible RFID-enabled document presented by the vehicle occupants, retrieves a unique tag identifier (ID), and transmits it to CBSA systems. Chips in RFID-enabled travel documents that are not accepted under the initiative will be automatically filtered out by CBSA systems. There is no personal information contained within the RFID chip; only the unique tag ID. When the unique tag ID is received by the CBSA systems, a process is activated to send a request to the relevant secure database. It is validated and the corresponding traveller tombstone information is retrieved from the database. This information will then populate the application and a risk assessment is performed prior to presenting the biographic information and query results to the BSO.

CBSA staff with access to GEC use passwords to access data and User Audits.

NEXUS kiosks use audit trails that can be used by the CBSA to ensure a user's actions can be traced back to that individual; various databases are accessed for query during a passage including Global Enrolment, RAC, ICES and GCMS. All database writes or modifications log the user's name and timestamp. A Kiosk-specific audit log is also created during the time of passage.

6.3.3 Use of automated personal information analysis, personal information matching and knowledge discovery techniques:

For the purposes of the Directive on PIA, CBSA is to identify those activities that involve the use of automated technology to analyze, create, compare, cull, identify or extract personal information elements. Such activities would include personal information matching, record linkage, personal information mining, personal information comparison, knowledge discovery, information filtering or analysis. Such activities involve some form of artificial intelligence

☒ YES
☐ NO

and/or machine learning to uncover knowledge (intelligence), trends/patterns or to predict behaviour.

Details: Data matching is used to eliminate inaccurate or duplicate information at enrolment and to risk assess applicants to ensure that existing NEXUS members remain in good standing. This is consistent with the stated purpose of data collection i.e. the administration of NEXUS, and this activity is disclosed to prospective applicants during the application/interview process.

A YES response to any of the above indicates potential privacy concerns and risks that need to be measured and mitigated.

G. Personal Information Transmission

Level of Risk

The personal information is used within a closed system.

☐ 1

No connections to Internet, Intranet or any other system. Circulation of hardcopy documents is controlled.

The personal information is used in system that has connections to at least one other system.

☒ 2

The personal information is transferred to a portable device or is printed.

☒ 3

USB key, CD-Rom, laptop computer, any transfer of the personal information to a different medium.

The personal information is transmitted using wireless technologies.

☐ 4

Details: NEXUS applications submitted via the U.S. GOES are transmitted to the CBSA via GEC and to the U.S. CBP's GES. Both countries then independently perform security queries and determine eligibility in the program. The information provided is stored in separate databases by both countries. Once approved by both countries (which includes attending an interview at an EC), the member's information is submitted to the U.S. GPO for printing of the NEXUS card. If applying by mail, the applicant downloads the NEXUS application, prints and completes it and mails it to the appropriate CPC for processing.

For the Trilateral Trusted Traveller Arrangement, no personal information is shared between the CBSA and Mexico's INM nor with the UK Border Force. A Third country national will apply to NEXUS. Upon completion of the NEXUS application, information is shared between the CBSA and U.S. CBP as per standard protocol. Additionally, USCBP will share the following fields with the "other Agency" at time of application: domestic program membership number; first name(s); last name(s); gender; date of birth; nationality; passport number; passport country of issuance; and, passport issuance and expiry date to confirm identity and determine membership in their own domestic program.

The CBSA and U.S. CBP independently determine an applicant's status and only share the "Pass" / "Fail" indicator.

H. Risk Impact to the CBSA

Level of Risk

Managerial harm.

☒ 1

Processes must be reviewed, tools must be changed, change in provider / partner.

Organizational harm.

☐ 2

NEXUS Program

PIA

Changes to the organizational structure, changes to the organizations decision-making structure, changes to the distribution of responsibilities and accountabilities, changes to the program activity architecture, departure of employees, reallocation of HR resources.	
Financial harm. Lawsuit, additional moneys required reallocation of financial resources.	<input type="checkbox"/> 3
Reputation harm, embarrassment, loss of credibility. Decreased confidence by the public, elected officials under the spotlight, institution strategic outcome compromised, government priority compromised, impact on the (GoC) outcome areas.	<input checked="" type="checkbox"/> 4
Details: If a privacy breach were to occur, the potential harm to the CBSA would be to suffer reputational harm, especially considering the Agency is considered a law enforcement body and, as part of the NEXUS program, is handling and processing possible criminal records and bio-data information that could be used to commit identity theft offences.	

I. Risk Impact to the Individual or Employee	Level of Risk
Inconvenience.	<input checked="" type="checkbox"/> 1
Reputation harm, embarrassment.	<input checked="" type="checkbox"/> 2
Financial harm.	<input checked="" type="checkbox"/> 3
Physical harm.	<input type="checkbox"/> 4
Details: As the NEXUS application includes sufficient bio-data to commit identity theft offences and includes possible criminal records information, a privacy breach could be harmful to individuals across three of the four levels of risk. If the privacy breach included information that would not be sufficient to commit identity theft or included criminal records, the loss would likely be limited to an inconvenience.	

SECTION 3 - ANALYSIS OF PERSONAL INFORMATION ELEMENTS

Personal Information Elements and Sub-elements

Note: Identification of sub-elements is necessary where sensitive personal information is being collected or where the type of program or activity presents a potential privacy risk at levels 2, 3, or 4 in "Section 2 - Risk Identification and Categorization" above.

Category Of Personal Information	Personal Information Element	Personal Information Sub-Element	Format	Purpose / Necessity of Element
<i>Name</i>	<i>Name</i>	<i>First name / middle initial / last name</i> <i>Nickname</i> <i>Other Names (former names, maiden names)</i>	<i>Paper and Electronic</i>	<i>To identify clients</i>
<i>Physical Attributes</i>	<i>Gender</i>	<i>Male/Female</i>	<i>Paper and Electronic</i>	<i>To identify clients</i>
<i>Date of Birth (DOB)</i>	<i>DOB</i>	<i>Month/Day/Year</i> <i>Birth Certificate Information</i>	<i>Paper and Electronic</i>	<i>To identify clients</i>
<i>Birth Certificate</i>	<i>Birth Certificate No. and Document</i>	<i>Birth Certificate No and Document</i>	<i>Paper and Electronic</i>	<i>To provide proof of citizenship and birth.</i>
<i>Place of Birth</i>	<i>Place of Birth</i>	<i>City/State or Province/Country</i>	<i>Paper and Electronic</i>	<i>To identify the individual and eligibility in the program.</i>
<i>Citizenship Status or Nationality</i>	<i>Citizenship Status</i>	<i>Citizenship in Canada or the United States;</i> <i>Citizenship and/or Nationality of Third Country that has an arrangement with CBSA-CBP NEXUS Program</i>	<i>Paper and Electronic</i>	<i>To provide proof of identity and citizenship/status.</i>

Category Of Personal Information	Personal Information Element	Personal Information Sub-Element	Format	Purpose / Necessity of Element
<i>Citizenship Status or Nationality</i>	<i>Citizenship Document Naturalization Certificate No and Document Visa/Permit Permanent Resident Document</i>	<i>Citizenship Document Naturalization Certificate No and Document Visa/Permit Permanent Resident Document</i>	<i>Paper and Electronic</i>	<i>To provide proof of identity and citizenship/status.</i>
<i>Passport Number or Travel Document</i>	<i>Passport or Travel Document Number (and photocopy of document)</i>	<i>Passport Number Travel Document Number Photocopy of document</i>	<i>Paper and Electronic</i>	<i>To provide proof of identity, citizenship, and to determine eligibility in the program.</i>
<i>Other Identification Numbers</i>	<i>Driver's License and Number</i>	<i>Driver's License and Number</i>	<i>Paper and Electronic</i>	<i>To provide proof of identity and to determine eligibility in the program.</i>
<i>Other identification Numbers</i>	<i>CBSA (GEC system driven number) CBP (GES system driven number)</i>	<i>GEC Identification number GES identification number</i>	<i>Paper and Electronic</i>	<i>To identify individual's by file number.</i>
<i>Contact information</i>	<i>Home address Previous Home address</i>	<i>Street name / street number / city / province or state / postal code/country/telephone number/business telephone number/email address From Date/To Date</i>	<i>Paper and Electronic</i>	<i>To contact clients and to assist in performing checks in determining eligibility in the program; to deliver NEXUS card</i>
<i>Biographical Information</i>	<i>Work History</i>	<i>Employer Name/street address/city/province or state/postal code/country Employer telephone number Type of Occupation From Date/To Date</i>	<i>Paper and Electronic</i>	<i>To assist in performing checks in determining eligibility in the program</i>

Category Of Personal Information	Personal Information Element	Personal Information Sub-Element	Format	Purpose / Necessity of Element
<i>Biometric Information</i>	<i>Iris Scan Photograph</i>	<i>Iris Scan Photograph</i>	<i>Electronic</i>	<i>To identify clients upon entry into Canada as being a trusted member of the program.</i>
<i>Credit Information</i>	<i>Credit Card Information</i>	<i>Credit Card Information</i>	<i>Paper and Electronic</i>	<i>To collect payment for inclusion in the program</i>
<i>Signature</i>	<i>Signature</i>	<i>Signature</i>	<i>Paper and Electronic</i>	<i>Collected along with the credit card information for payment purposes To record certification that application information provided is accurate</i>
<i>Criminal Checks/History</i>	<i>Criminal Checks/History</i>	<i>Criminal History Information</i>	<i>Paper and Electronic</i>	<i>To determine eligibility in the program</i>
<i>Immigration enforcement history</i>	<i>Immigration Checks/History</i>	<i>Immigration History Information</i>	<i>Paper and Electronic</i>	<i>To determine eligibility in the program</i>
<i>New Fields for Trilateral Trusted Traveller Arrangement</i>				
<i>Other identification Numbers for Third Country Applicants</i>	<i>Confirmation that an applicant is a member of their own trusted traveller program (done through GOES by U.S. CBP)</i>	<i>Yes/No</i>	<i>Electronic</i>	<i>To determine eligibility</i>
<i>Visa Number</i>	<i>Visa Number Photocopy of Visa</i>	<i>Visa Number Photocopy of Visa Electronic Travel Authorization</i>	<i>Paper and Electronic</i>	<i>To provide proof of identity, citizenship, and to determine eligibility and admissibility in the program.</i>

Note: **Category of personal information:** TBS has developed a list of categories of personal information to simplify the process of describing personal information in Personal Information Banks (PIBs). It provides examples of categories and elements that can be used to summarize the personal information collected by most federal institutions. The CBSA ATI and Privacy Division has modified the list to better reflect CBSA business lines. The list can be found in Annex C.

Personal information element: Identify each element of personal information collected (for example: 1) name, 2) home address).

Personal information sub-element: Identify sub-elements associated with each element of personal information collected (for example: 1) first name / middle initial / last name, 2) street name / street number / city / province / postal code).

Type of format: Identify how the personal information will be recorded: on paper, electronically, audio recordings, visual image recordings, human biological samples or other (specify).

Purpose of the personal information: Indicate the purpose for which you are collecting these elements or sub-elements of personal information and how these are necessary for the program or activity (Note: "necessary" is a higher standard than merely being useful.)

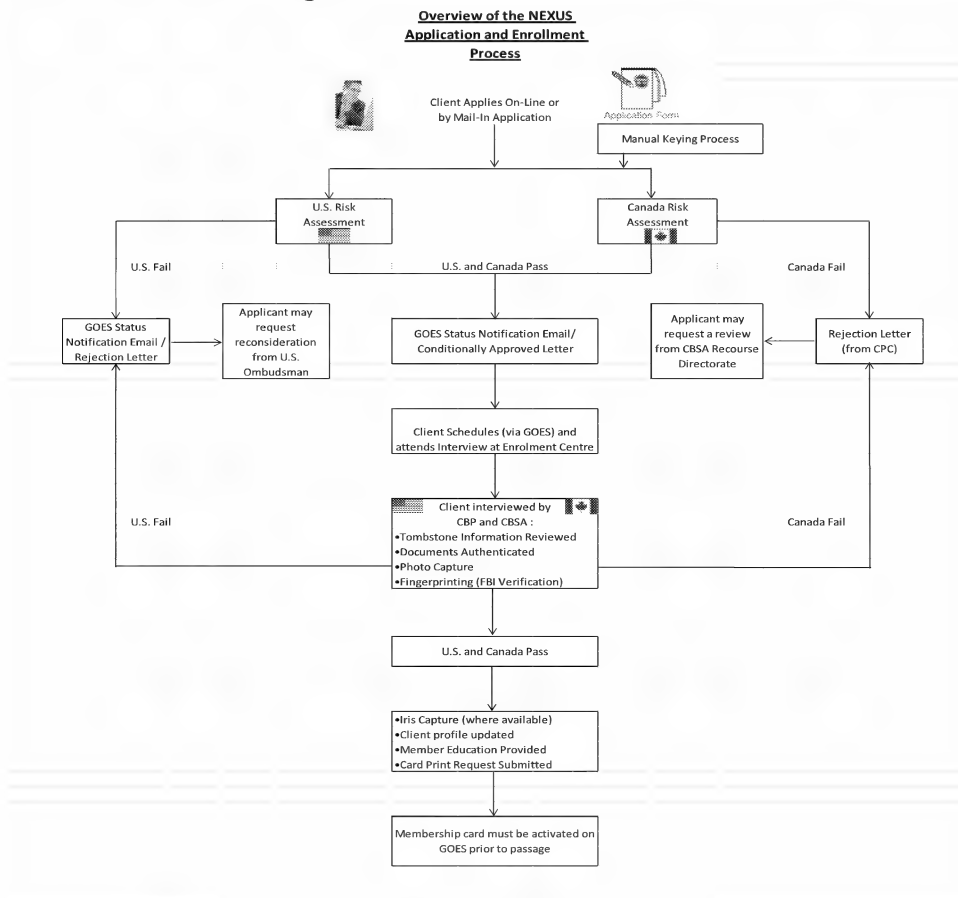
SECTION 4 - FLOW OF PERSONAL INFORMATION

4.1. Information Systems

In this section list and describe the information systems involved in the NEXUS application and processing work flows. For each system, describe the following:

- Overall function of the system within CBSA
- Function/Use of the system within CBSA
- Description of the personal information stored in the system related to NEXUS
- How it is used to support the NEXUS Program
- Restrictions within the system, such as user rights, read only, etc.
- Audit capabilities

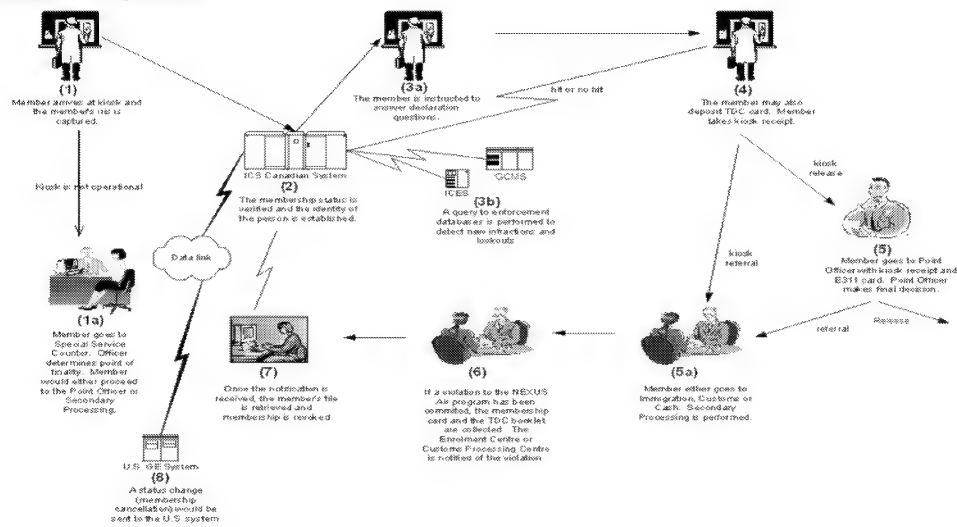
Data Flow Model – Diagram



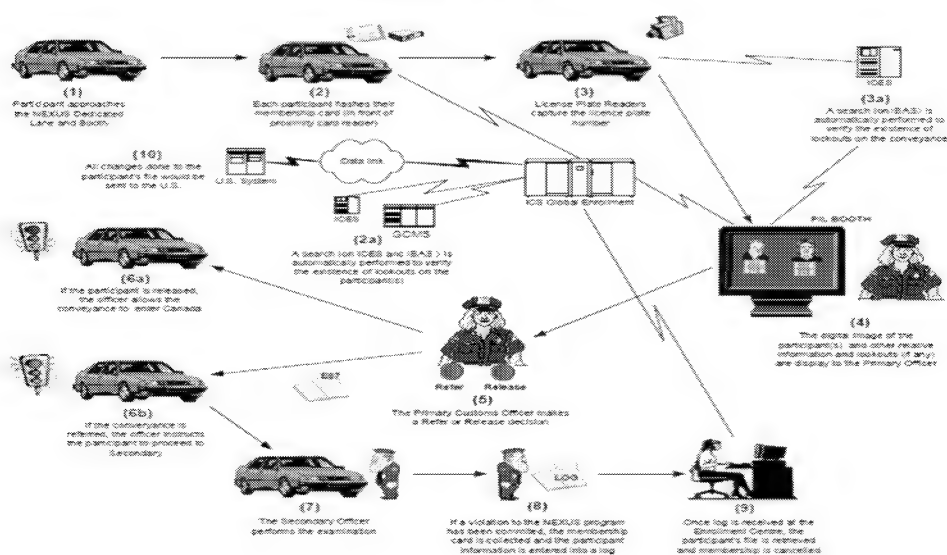
Trilateral Trusted Traveller Arrangement:

The only “change” here is that the US system will check with the Mexican DB to ensure that the applicant is in fact a member of their domestic program with a Yes/No confirmation. Third country nationals will not be able to apply through paper application.

Air Passage

Diagram 2:
Passage (Entering Canada)

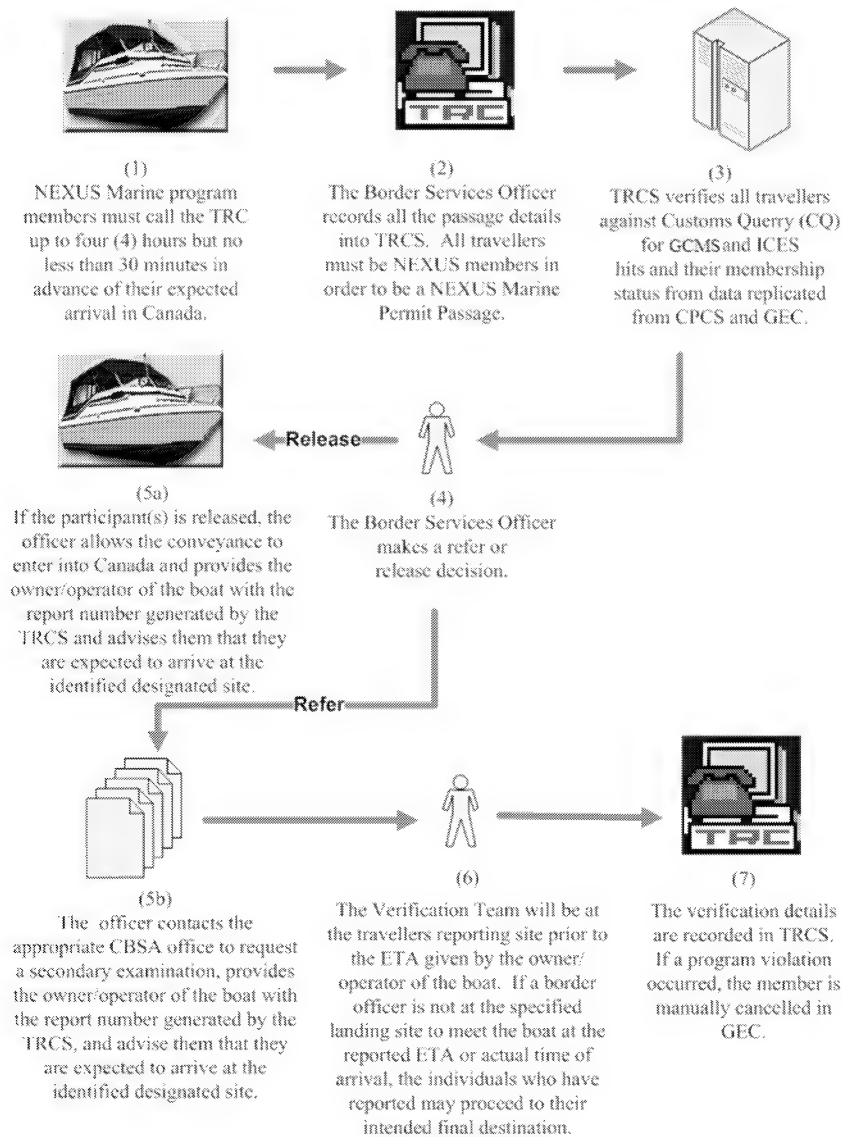
NEXUS Highway Passage



Trilateral Trusted Traveller Arrangement:

The only changes in the highway passage will be that the member will need to validate their visa validity for visa-required countries and validate their eTA for air passage. Note, third country nationals do not receive benefits in the marine mode.

NEXUS Marine Passage

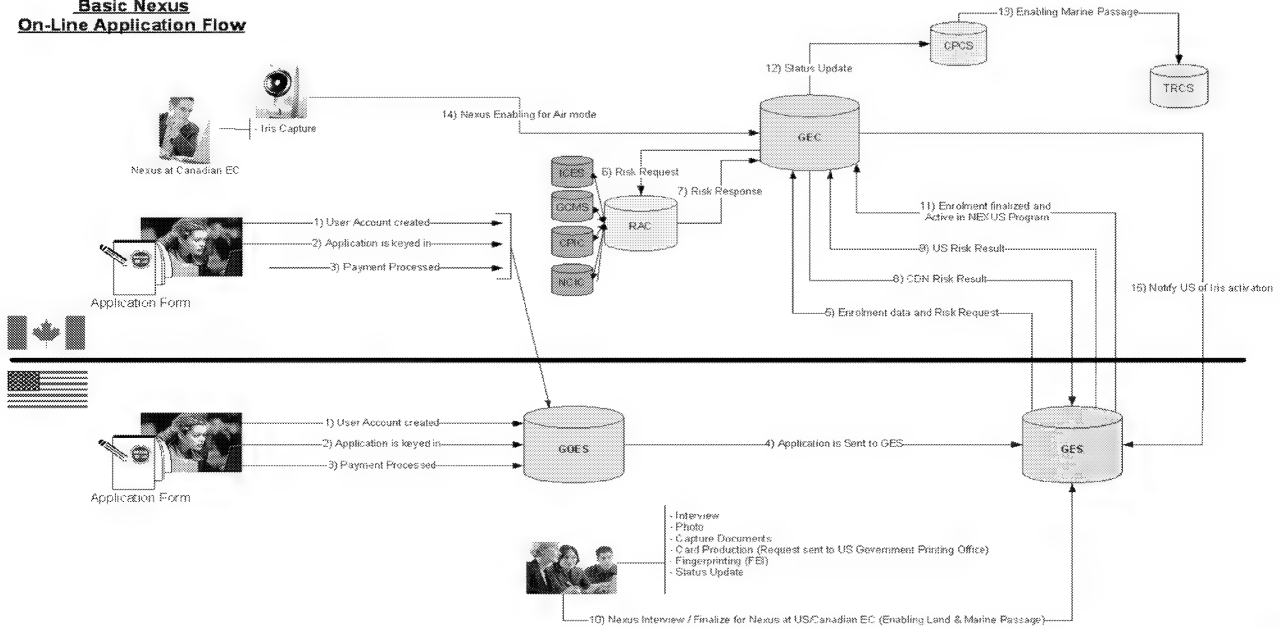


NEXUS Program

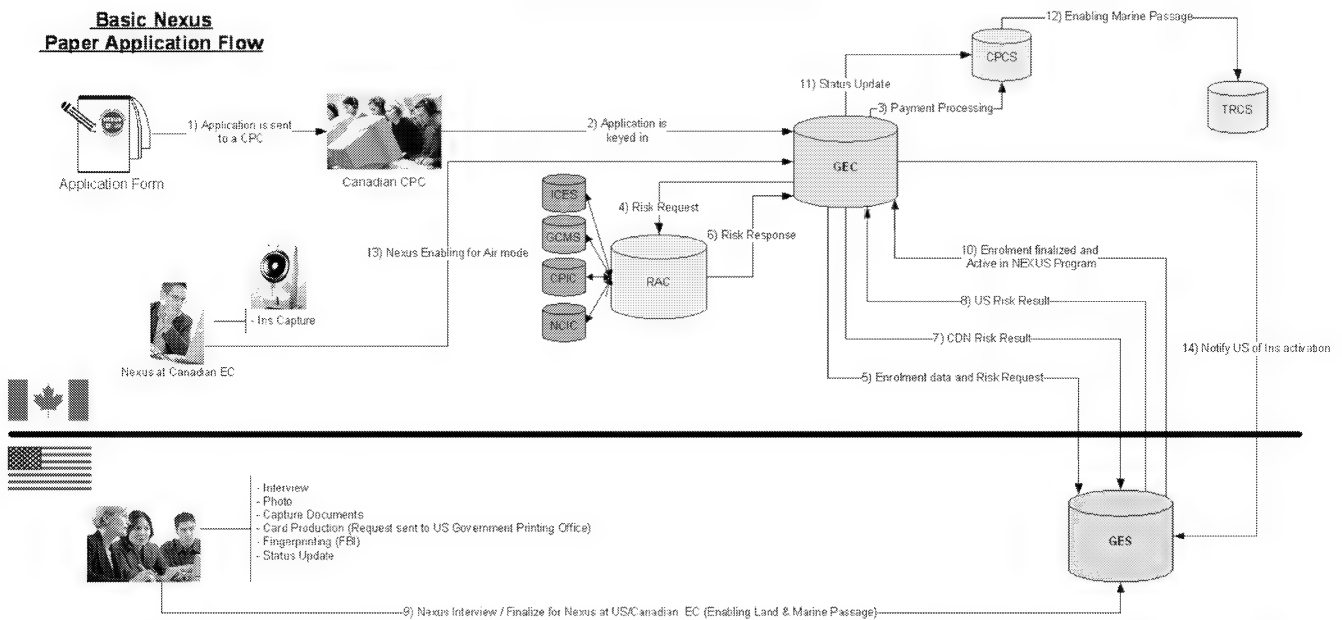
PIA

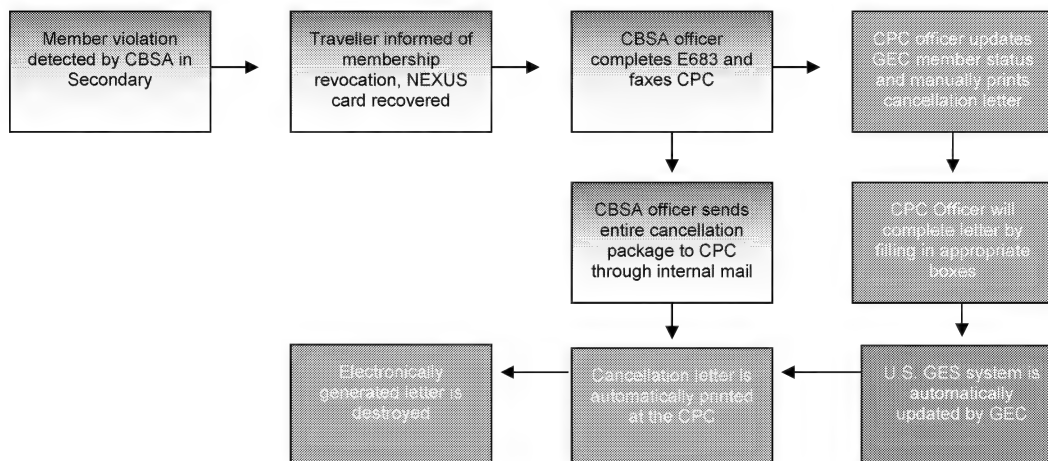
Basic Nexus On-Line Application Flow

NEXUS - On-Line Application Flow

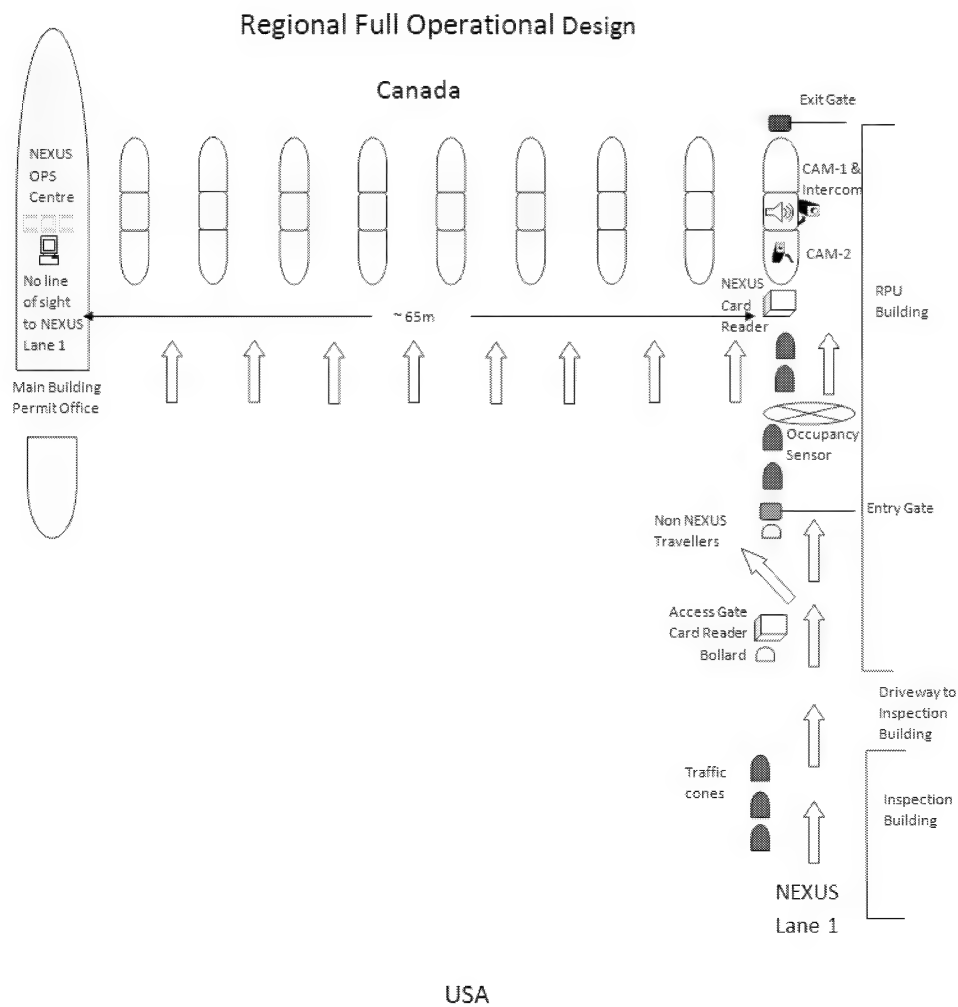


NEXUS - Paper Application Flow



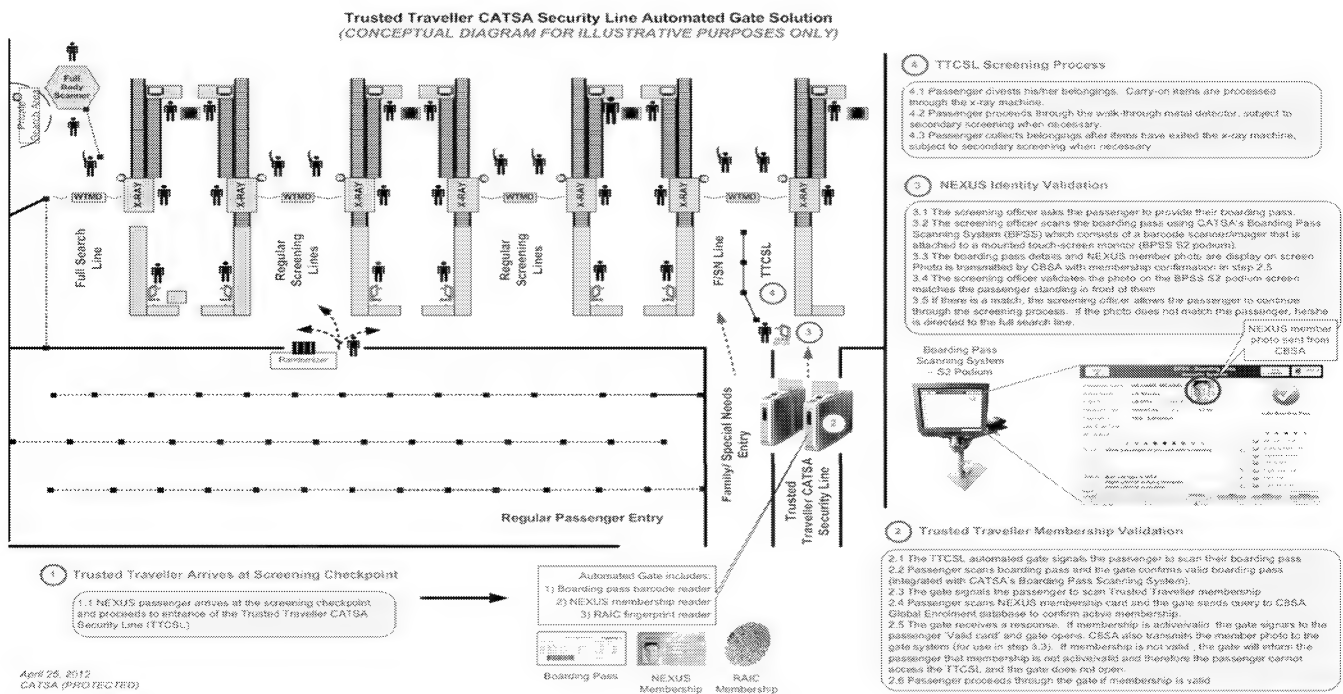
CBSA Revocation of NEXUS Privileges Flowchart

E- GATE



NEXUS Program

PIA

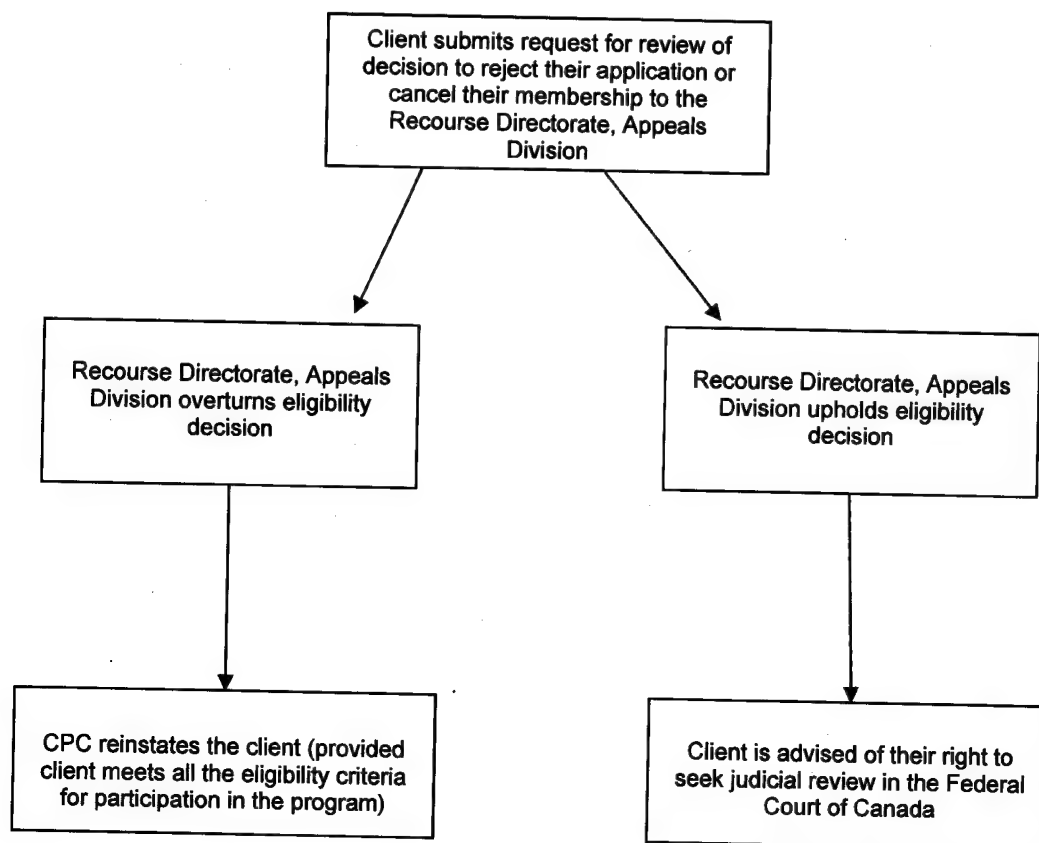


April 25, 2012
 CATSA (PROTECTED)

Canada Border Services Agency

49

REDRESS FOR TRUSTED TRAVELLER PROGRAMS



1. GEC/CPCS

NEXUS membership data is captured and stored on the CBSA's GEC. GEC is a component within the Integrated Customs System (ICS) that provides the key infrastructure component for the delivery of trusted traveller programs by capturing the application data. The personal information entered by the applicant is used by the CBSA to determine the eligibility of the applicant and to confirm their identity. The personal information elements are listed in Section 3. CPCS is the Canadian system that stores payment transactions for NEXUS.

Audits and compliance checks are not regularly scheduled for user activity in GEC/CPCS, nor are there any plans to establish these measures in the future.

The risk of unauthorized user activity in GEC/CPCS is minimal since modifications are tracked by user ID, time of the change, user profiles, and firewalls which restrict unauthorized access.

Access to data records is determined through user profiles. User profiles are used to govern the control and administration of personal and payment information. Only system administrators and authorized CBSA maintenance personnel have access to all data for system maintenance purposes. The number of privileged maintenance users is kept to a minimum. These employees are security screened to the appropriate level and receive security awareness training. Moreover, users are limited to accessing only data and services for which they have been authorized. To ensure users are accessing information appropriately, log records are maintained of all user access and any modifications to an individual's record. These records may be used for audit purposes.

2. Iris database

An iris scan is performed at a NEXUS kiosk upon return to Canada. The scan at the kiosk is not stored by the CBSA; it is only matched with the stored iris that the CBSA would have taken at NEXUS enrolment. The purpose of the iris database is for identity matching.

The Iris Matcher Server is an iris identification piece of technology. It manages the iris templates and iris comparison software. It is responsible for handling client kiosk requests to analyze irises and return an identifier associated with the request.

The various components of ICS that are in play when the kiosk is accessed reside partially on the mainframe servers and partially on a WebSphere server. The components reside within a secure area at Headquarters.

3. Third Country Database

No personal information is shared directly between the CBSA and the third country since the third country applicant applies directly through GOES who then sends the applicant's information to the CBSA through GEC for a NEXUS risk assessment (but only if the applicant is a member of their own domestic program). The same applies in reverse; a Canadian citizen who is a NEXUS member would apply directly to the third country program. The U.S. confirms the identity and NEXUS membership through a connection with the third country's IT system.

4. NEXUS eGate

It was determined that the use of the NEXUS eGate would provide NEXUS members extended access to the NEXUS lane after scheduled hours of operation at the POE, without increasing risk, and providing flexibility in terms of resource management by giving BSOs the ability to perform other duties inside the office, while awaiting NEXUS traffic. The NEXUS eGate lane is operated remotely from inside the CBSA office at the POE. There are no information sharing considerations outside the regular operation of the CBSA.

5. NEXUS Kiosk Replacement and Expansion

The Kiosk Replacement and Expansion Plan saw 86 new NEXUS kiosks being installed to address the ageing technology and kiosk reliability issues. The new kiosks are equipped with document readers, dual printers and updated iris cameras and touch screens, which were purchased and implemented starting in fall 2014. This innovative solution has improved the NEXUS client experience and enhanced the integrity of the NEXUS program. There are no information sharing considerations outside the regular operation of the CBSA.

Kiosk usage is recorded for complete passages, as well as incomplete passages (i.e. timeout of the session, irises not read properly, system error, session cancelled by traveller, inactive membership, document reader failure) for identified members (date, location, screen message generated). In the case of an incomplete passage, NEXUS members would use the Special Services Counter. Complete and incomplete passages would be used for the purposes of auditing the frequency of these events. There is an audit trail of referrals that are stored in passage history in ICS. This database will only store one referral type per area i.e. one customs and/or one immigration referral type. However, it will store all reasons for the referral.

The overall process of kiosk use remains the same:

- Kiosk processes one member at a time.
- The individual must be a NEXUS member before they can have access to the air passage process.
- Kiosks for entry to Canada recognize NEXUS members. Unidentified users are instructed to use regular lanes.
- Members are allowed to use kiosks in any location in Canada where kiosks are available. Kiosks are located in the Customs Hall in Canadian international airports.
- Passage must be accessible and operational 24/7. If the system is down NEXUS members may use the Special Services Counter to enter Canada.
- Ability to provide passage clearance within a set amount of time, otherwise must direct members to appropriate alternative process.
- Member must carry a valid NEXUS card
- Membership must be in "active" status.
- The kiosk instructs the member (using a video) on how to present their document to the reader.
 - Authorized document: NEXUS membership card.
- The kiosk verbally and visually instructs the member on how to submit their iris biometric to confirm identity.

- Member must have a NEXUS membership card and an iris enrolment reference stored in the enrolment database to access the passage process at a kiosk;
 - Members with a permanent medical condition preventing the successful capture of their iris biometric will still be allowed membership in NEXUS.
 - Members meeting the above criteria are to have an 'active' membership status with a reason code indicating no biometric captured.
 - Members with a temporary medical condition preventing the successful capture of their iris biometric, such as cataract surgery, will be allowed membership in NEXUS same as above, but will be asked to return to an enrolment centre within a designated period of time (e.g. 6 months) to attempt another capture.
- Membership validation via membership card is required to access the passage process at a kiosk.
- At time of passage, the system displays 'passage questions' and prompts the member to answer each of them.
- All members who are granted passage at the kiosk, are issued a receipt identifying the member's name, residency, membership ID, date & time of passage, kiosk ID and work location, and referral/release code.
 - For a particular identified member, save details of kiosk usage at a given date, time, work location, kiosk/lane.
- Depending on transactions at passage and how the questions are answered, the member is referred to the appropriate authority with a printed receipt.
- The system provides general kiosk usage statistics such as national usage for all kiosks, including on an individual member basis.
- Kiosk usage is recorded for complete passages, as well as incomplete passages (i.e. timeout of the session, irises not read properly, system error, session cancelled by traveller, inactive membership, document reader failure) for identified members (date, location, screen message generated). In the case of an incomplete passage, NEXUS members would use the Special Services Counter. Complete and incomplete passages would be used for the purposes of auditing the frequency of these events. There is an audit trail of referrals that are stored in passage history in ICS. This database will only store one referral type per area i.e. one customs and/or one immigration referral type. However, it will store all reasons for the referral.
- Eastern timestamp is used when storing date time elements. Reports and retrieval of passage data should be in local time zone. Local time zone should be available for *ad hoc* reports.
- Any Selected Other Government Departments (SOGD) questions which are in addition to the regular questions contained within Part A of the Declaration Card (E311 form), will, as required, be added to the Canada-entry kiosk questions.
- After kiosk passage has been successfully completed, the member will receive a kiosk receipt to present to a point officer to exit the Customs Hall.
- Kiosk displays a screen message instructing the member to remove their membership card and receipt before proceeding to the designated area.
- The kiosk or receipt printer emits a warning sound i.e. continuous beep until the member has taken the receipt from the kiosk.

- An immigration referral is generated for immigration documents that have expired or are expiring within 10 days of passage.
- If a kiosk passage cannot be completed for specifically defined reasons, the kiosk displays a screen message to direct the member to the appropriate designated area.
- CBSA HQ designated program personnel sets the required referral codes.
- Passage is only complete when the control/point officer makes a final decision.

In terms of auditing, a BSO will add the identification, date and time to the following events and keep the information in a centralized location when the following stored data elements are viewed or modified, including client logon and logoff times:

- Client information
 - Changes of saved personal data will be tracked
 - Changes to the personal information of the client - noting the date and time of the data change will allow for tracking what is changed since the past values are to be kept for a period of five years
 - Each time the client account information is viewed by a program administrator, Audit Trail information will be retained
- Risk Assessment
 - Audit information retained for any client status updates
- Communications
 - Audit information retained for e-mails sent to each individual
 - Bulletins posted
- Schedule an Interview
 - Date and time and identification of when the schedule was made and, when applicable, cancelled

6. Trusted Traveller CATSA Security Lines (TTCSL)

A pilot of the TTCSL automated gate solution using RFID technology to validate NEXUS memberships, is being conducted at the domestic/international pre-board screening checkpoint at the Edmonton International Airport. At this pilot site, NEXUS members tap their card at the RFID reader on the eGate to confirm their membership is valid rather than visual card verification by a CATSA security officer (verification method performed at all other CATSA pre-board screening checkpoints that validate NEXUS members to access the TTCSL). The CBSA and CATSA jointly use RFID technology solely at the Edmonton International Airport pilot site and not at other CATSA screening checkpoints for NEXUS members accessing the TTCSL. When a NEXUS member uses the dedicated CATSA line at the Edmonton domestic/international pre-board screening checkpoint, he/she uses the RFID embedded in the card that will prompt a picture of the member associated with that card on a screen for a security officer to view and match the person using the CATSA line. If the screening officer deems it to be a match, the officer allows the member through the gate; if it is not a match, the person is sent to the regular security screening line. Nothing more than the person's photo is displayed to the security officer in order to verify the NEXUS member at the CATSA line. After the photo is viewed by the screening officer, the CATSA information system permanently deletes the photograph. The CBSA has made in-house system changes to allow CATSA to ping the GEC database which houses NEXUS membership data. Signage has been

placed on top of the screen monitor that informs the passenger that CATSA will verify their NEXUS credentials with CBSA if the passenger uses the TTCSL.

CATSA is planning to roll out an automated gate solution with NEXUS card validation functionality (RFID) at the new Calgary International Airport terminal in January 2017.

The pilot is continuing in Edmonton and an MoU for the disclosure of NEXUS information to CATSA to enable CATSA to develop and maintain a TTCSL Automated Gate Solution with the CBSA has been developed. An SLA has also been signed between the CBSA and CATSA. Both documents expire on December 31, 2016.

There is an audit of all requests and replies for the Enrolment Query Service.

7. RFID

In the NEXUS land mode, Vicinity RFID allows an RFID chip to be read within three to four metres of an RFID antenna. The antenna is activated to read the chip when a sensor is triggered by the approach of a vehicle in an RFID-enabled NEXUS lane. Once activated, the antenna reads the chip in the eligible RFID-enabled document presented by the vehicle occupants, retrieves a unique tag identifier (ID), and transmits it to CBSA systems. Chips in RFID-enabled travel documents that are not accepted under the Initiative will be automatically filtered out by CBSA systems.

There is no personal information contained within the RFID chip except for the unique tag ID. When the unique tag ID is received by CBSA systems, a process is activated to send a request to the relevant secure database where it is validated, and the corresponding traveller tombstone information is retrieved. This information then populates the BSO's screen and a risk assessment is performed on the driver and any passengers.

An IT update was made to the Integrated Primary Inspection Line (IPIL) Highway traveller processing application in October 2014, allowing NEXUS cards to be read by existing RFID-readers in flex lanes.

Explanation of the process.

Ensure that the work flows provide a description of the data elements and work flows. As reflected in the CBSA response to the OPC in Oct 2012:

When a Canadian applicant applies to the NEXUS program, he/she can do so through either paper application in Canada or electronically through the U.S. GOES portal. Through paper application, the personal information collected on the form is entered manually in the Canadian GEC of the ICS which connects with the U.S. GES. This way, personal information provided by the applicant is provided to both governments for risk-assessment. Through an electronic application processed through GOES, the principle is very similar in the sense that the applicant provides his/her personal information by keying it into GOES which provides the information to both governments through its links to the U.S. GES which is linked to the Canadian GEC. On both the paper and electronic application forms there are Privacy Statements for Canada and the U.S. which describes the purpose for collecting the information and the fact that the information may be shared with other government agencies.

An applicant's personal information is risk assessed independently by Canada and the U.S. (see above for data elements checked and procedure used for the risk assessment in Canada). Therefore, no data elements or other personal information are disclosed to any U.S. agencies from the CBSA for NEXUS eligibility assessment purposes. Once the U.S. CBP has completed their separate eligibility assessment, they will simply provide a "Pass" / "Fail" indicator. After independent risk assessments, Canada provides the same indicator to the U.S. CBP. No reason(s) or rationale for a "Pass" or "Fail" is provided.

The U.S. may disclose information in accordance with their privacy legislation. In the case of the CBSA, the disclosure must be in accordance with section 107 of the *Customs Act* and that in the case of the U.S. CBP, it must also be in accordance with the *Freedom of Information Act* (FOIA). Should there be a disclosure to third parties, it must first be done by obtaining the written permission of the sending country, except if the disclosure is done in order to obtain assistance from the third party on the assessment of an application.

As part of the trilateral trusted traveller arrangement, third country nationals will only be able to apply to NEXUS electronically through the U.S. operated GOES.

Identification Numbers

Each NEXUS member is assigned the following unique personal identifiers:

- CBSA (GEC system driven number)
- CBP (GES system driven number)
- CPCS (payment transaction number when appropriate)

These numbers are used to cross reference NEXUS clients across various databases to support the delivery of the NEXUS program as well as to eliminate duplicate applications/documents.

An activity log is maintained of all transactions made on an individual's membership record.

Risk Assessments

Risk assessments are conducted prior to membership approval, at passage and again on a regularly scheduled basis (once a year or on an *ad hoc* basis) during the term of a NEXUS membership. These risk assessments use personal information collected by other agencies, including law enforcement and other government departments to determine eligibility to participate and retain NEXUS program membership. During these risk assessments, an applicant's personal information is not disclosed to other Canadian Federal Government institutions. Rather, the CBSA uses the personal information such as surname, middle name, given name, maiden name, DOB, and address to query information from other institution's databases to which the CBSA has access. The CBSA also queries its own databases. For all searches, the least amount of information is entered into the search function of the database being used.

Specifically, four databases are queried during the risk assessment stage:

1. IBAS
2. CPIC
3. ICES

4. NCIC

These databases reveal if the person has any recorded violations/contraventions of any of the program legislation enforced by the CBSA, in particular the *IRPA*, the *Customs Act*, the *Criminal Code of Canada*, and the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA)* which may exclude the applicant from the program. The NEXUS terms and conditions are found at the following link: <http://www.cbsa-asfc.gc.ca/prog/nexus/term-eng.html>

NCIC is the U.S. equivalent to CPIC, which houses wants/warrants and criminal records, and is used by the CBSA to determine if a crime committed or a want/warrant issued in the U.S. would be equivalent (in terms of seriousness) in Canada. For example, certain crimes in the U.S. that may not be considered serious enough to exclude an applicant from the program in the U.S. may be considered a serious crime in Canada, and vice versa.

Credit Card Information

Applicants have the option of paying for the application processing fee by way of a credit card. This option also requires the applicants' consent. Credit card information is maintained in the CPCS. Access to this sensitive financial information is limited to CBSA users involved in membership enrolment, status updates, renewals, and monitoring of NEXUS program trends by headquarters staff. Each user is assigned an identifier and all transactions are logged. As well, Canadian residents who use a Traveller Declaration Card (TDC) voluntarily provide their credit card information when submitting their TDC. The CBSA's Policy on the Retention of Payment Card Information for Trusted Traveller Programs is attached at Schedule J.

Credit card information collected by the CBSA when a paper application is processed is not shared with any other business application at the CBSA or other government department. Likewise, CBP does not share the credit card information with the CBSA when this information is provided via the GOES on-line application.

Biometric Information

Biometric information is collected at the time of enrolment. The iris scan is used to identify the member at air passage. A photograph is also used to identify the member at land passage and during the eGate pilot. Fingerprints are collected by the U.S. CBP to verify the identity of the member during initial enrolment, renewal or re-enrolment. These fingerprints are not shared with the CBSA.

The personal information collected to determine membership eligibility includes biometric data and it is captured at two points: at enrolment, and again at each passage. A record of the iris image captured at enrolment is retained in the Iris Storage Database. The passage image is a transitory record used to compare against this stored image to establish a match. No new iris biometrics are collected at time of membership renewal. As part of the NEXUS enrolment process, an applicant interview takes place where both the CBSA and CBP are represented. This interview process consists of a review of all documents for authenticity, of client contact information and an explanation of the reporting requirements for each of the interviewers' respective countries. Notes may be made in the general note area of GEC and GES of each respective country.

Notice

The individual must sign a statement of consent on the application form to the collection, use and sharing of personal information, or indicate agreement to a statement of consent if using the online enrolment system. Consent is also obtained on the TDC form. With respect to minors, there is a standard mechanism in place to ensure the recognition of persons authorized to make decisions on behalf of others. The NEXUS application form states: "If applying for a child under 18 years of age, you must ensure that you provide documentary evidence that you have authority to apply on behalf of the child and that a photocopy of all legal documents regarding custody are submitted." In such circumstances the parent or guardian must present this documentary evidence to the CBSA and U.S. CBP officers during the interview at the EC.

Pursuant to sections 7(2) and 7(2.1) of the *Presentation of Persons (2003) Regulations*, a person may apply for an authorization (e.g. NEXUS card) on behalf of a child who is under 18 years of age or on behalf of a person over the age of 18 who has a mental or physical disability, respectively. Should an applicant mentioned above pass the initial application process, the person applying on behalf of the applicant will normally accompany that person to the interview at the EC. Their capacity to act on behalf of another individual may be further assessed at the interview.

The NEXUS website (www.nexus.gc.ca) does provide information on using a third party representative to apply for the program.

As reflected in the CBSA's October 2012 response to the OPC, the Privacy Notice Statement (PNS) for the NEXUS application has been modified to provide a more thorough description of the legal authority and uses of information provided to the CBSA by applicants. The revised PNS is as follows:

Canada's Privacy Statement

The information you provide in your application, including supporting documentation and biometric data, is collected by the Canada Border Services Agency (CBSA) and is protected pursuant to both the *Customs Act* and the *Privacy Act*. In accordance with Canadian laws and regulations, this information will be shared with other government departments or agencies in Canada and the United States of America for the purpose of the operation of the NEXUS program and to conduct applicable checks and verifications to determine your eligibility and continued eligibility in the NEXUS program. If the required information is not provided, your application may not be processed and the authorization may not be granted.

Individuals to whom the information relates have rights of access to, correction of and protection of, their personal information under the *Privacy Act*. The information collected is described in Personal Information Bank # CBSA PPU 031. Instructions for obtaining information are provided in Info Source, which is available at public libraries, government public reading rooms and on the Internet at: <http://infosource.gc.ca>

Correction of Information

Currently, when a NEXUS member wishes to correct or update their membership information (e.g. change in address or name) they may:

- Request the correction/update via GOES;
- Contact an official working at a NEXUS EC or CPC to request the correction or update; or,
- Submit a renewal/re-application that contains corrected/updated information.

4.2. Audit of NEXUS Use

Each time that NEXUS membership is modified in ICS, an audit trail is established that tracks user identification, date modified and field(s) modified. An audit trail is not recorded when data is merely accessed for review purposes; privacy risks of an unauthorized person accessing the system are minimized through security and training given to authorized ICS users. Compliance reviews are not currently being done to determine if authorized ICS users are accessing NEXUS membership information. Nevertheless, with the safeguards in place, the risk of compliance being abused or misused is considered minimal.

There is also an audit of CATSA use.

4.3. Retention of NEXUS Data

The retention period for NEXUS information, in line with the *Privacy Act* and its regulations, *Canada Evidence Act* and *Customs Act*, is as follows:

- Electronic and paper applications are destroyed according to the following schedule:
 - Refused applications for NEXUS: The application forms and accompanying documents will be destroyed two years after the redress period has expired if there has been no request for redress. This information is kept in order to satisfy *Privacy Act* requirements to keep personal information for two years following the last administrative use, and to allow the refused applicants the opportunity for redress.
 - Successful applicants for NEXUS: All paper application forms are scanned and then destroyed in accordance with the CBSA Records Retention and Disposition policy. Payment forms are not scanned and all physical copies are stored securely in case of payment dispute/refund request as per standards governing the handling of financial documents. The application form and electronic copies will both be destroyed six years after the date on which an application is approved. The retention period for the accompanying documents is still under development.
- Biometric information will be destroyed according to the following schedule:
 - Refused applicants to NEXUS: Failed applicants will not be asked to provide any biometric data.
 - Successful applicants to NEXUS: Only approved members are required to provide a photograph, and fingerprints (which are collected only by the U.S. CBP and are not shared with the CBSA). The iris biometric is optional, as this biometric is only

useful if the member wishes to use self-serve kiosks in airports. The retention period for the photograph and the initial iris scan taken at the time of enrolment is four years following the last time the information was used for an administrative purpose. Iris templates used to identify a member at time of passage are kept for a period of two years following each passage.

- With respect to kiosk receipt following the use of the self-service kiosks in the airports, it has been established that the CBSA does not have a legal obligation to retain the printed kiosk receipts because the receipt information is electronically collected.

The personal information described above is not shared externally.

A retention policy on Trusted Traveller Program's application forms has been developed as part of the Policy on the Retention of Payment Card Information (Schedule J). User activity of GEC and the CPCS within the CBSA can be monitored since the user making the modifications to data and the date and time of the modification are logged. Firewalls are used to protect the integrity of the data storage. Once information is modified by either the CBSA or the U.S. CBP, this information will be updated to other agencies' internal systems.

Audit records are retained and disposed of according to CBSA information management policies, and specifically Government of Canada multi-institution disposition authorities and CBSA institution-specific disposition authorities.

4.4. Data Flow Model - Table

SOURCE	IDENTIFY THE SOURCE
The individual or a representative	Individuals participating in the program
A federal government institution (identify from what PIB the information is obtained)	RCMP - Information Centre Database (RCMP PPU 005) IRCC - Interdiction Border Alert System (CIC PPU 042) CATSA – Boarding Pass Security Screening (CATSA PPU 100)
Non-federal institutions	
- Provincial Government	N/A
- Municipal Government	N/A
- Aboriginal Government / Council	N/A
- Organization of a Foreign State	U.S. CBP U.S. Government Printing Office (for the printing of the NEXUS card)
- International Organization	N/A

Private Sector	
- Located in Canada and Canadian Owned	N/A
- Located in Canada and Foreign Owned	N/A
- Located abroad and Canadian Owned	N/A
- Located abroad and Foreign Owned	N/A

4.5. Internal Use and Disclosure

Where will the information circulate within the CBSA? Identify any related programs or activities and personal information banks as identified in the CBSA Info Source chapter.

Program	Personal information bank
Travellers Programs: NEXUS Trusted Traveller Processing Integrated Customs Enforcement System Enforcement and Intelligence Operations Directorate Enforcement and Trade Appeals Operations – Overt Audio-Video Surveillance	CBSA PPU 031 CBSA PPU 1101 CBSA PPU 016 CBSA PPU 018 CBSA PPU 005 CBSA PPU 1104

4.6. External Use and Disclosure

The individual or a representative	
RCMP - Information Centre Database	RCMP PPU 005
IRCC - Interdiction Border Alert System	CIC PPU 042
CATSA – Boarding Pass Security Screening	CATSA PPU 100
Non-federal institutions and private sector	
- Provincial Government	N/A
- Municipal Government	N/A
- Aboriginal Government / Council	N/A
- Organization of a Foreign State	U.S. CBP/ U.S. GPO
- International Organization	N/A
Private Sector	
- Located in Canada and Canadian Owned	N/A
- Located in Canada and Foreign Owned	N/A

NEXUS Program

PIA

- Located abroad and Canadian Owned	N/A
- Located abroad and Foreign Owned	N/A

4.7. Retention / Storage

A federal government institution	CBSA
A Federal Records Centre	Back-up tape (3"x 3" disc) is physically stored with Library and Archives Canada for 6 years
Non-federal institutions and private sector	
- Provincial Government	N/A
- Municipal Government	N/A
- Aboriginal Government / Council	N/A
- Organization of a Foreign State	U.S. CBP U.S. GPO Mexico's Instituto Nacional de Migracion and the UK Border Force (no personal information is shared between the CBSA and these other organizations)
- International Organization	N/A
Private Sector	
- Located in Canada and Canadian Owned	N/A
- Located in Canada and Foreign Owned	N/A
- Located abroad and Canadian Owned	N/A
- Located abroad and Foreign Owned	N/A

4.8. Other Possible Considerations

Identify the areas, groups and individuals who access and handle the personal information:

The CBSA responsible for program or activity: There are 1,762 CBSA officers that have access to the NEXUS membership personal information and are responsible for the program or activity:		
Identify Groups or Areas / or Divisions	Positions who have access or use the personal information (where appropriate)	Geographical Location
Operations Branch, CBSA	Border Services Officers at any of Canada's eight international airports and Billy Bishop Toronto City Airport and at land ports of entry	Vancouver, Calgary, Edmonton, Winnipeg, Ottawa, Toronto, Montreal, Halifax and at NEXUS land POEs
Recourse Directorate	Appeals Analyst	National Capital Region
Program and Policy Management Division	Some Managers, Senior Program Advisors and Senior Program Officers to respond to internal queries or from the public	National Capital Region
Business Systems Integration Division	Some Managers, Senior Program Advisors and Senior Program Officers for production support purposes and troubleshooting; Help Desk inquiries	National Capital Region
Stakeholder Engagement & Outreach	Senior Program Advisors, Senior Program Officers and Junior Program Officers	National Capital Region
Other federal government Institution responsible for program or activity: (one table per institution):		
Non Federal Institution or Private Sector: 'name': (one table per institution)		

SECTION 5 - PRIVACY COMPLIANCE ANALYSIS

1. Legal Authority For Collection Of Personal Information

Has a legal authority been identified for the collection of personal information for this program or activity?

Statutory reference: Section 4 of *Privacy Act* (Section 4 has been interpreted to mean that a legal authority must be established for a collection of personal information, but section 4 does not provide legal authority for such a collection).

Policy reference: Section 6.2.6 of *Directive on Privacy Practices*

Yes

- 1.1 ☒ Specify the legal authority and briefly explain its connection to the program or activity or how it permits the collection of the personal information:

****Ensure that the legal authority to collect the personal information is cited in the relevant PIB and in "Section 1 – Overview and PIA Initiation" above.**

The NEXUS program is authorized under subsection 11.1(1) of the *Customs Act* and is also governed by the *Presentation of Persons (2003) Regulations*.

- 1.3 ☒ Is the personal information collected directly related to an operating program or activity?

Details: Personal information data will be used for the purposes for which the CBSA originally collected the data, that is, to make a determination on the applicant for membership eligibility and continued eligibility either during initial enrolment or at membership renewal as well as for the administration of the individual's membership record during the period of their participation in the program.

→ Continue to Question 2

No

- 1.3 ☐ If there is no legal authority for the collection of personal information, it cannot be collected. Please consult your legal advisor to determine if there is authority to proceed with the program or activity. ****The PIA process must not continue without this key information.****

2. Necessity To Collect Personal Information

Is each element and sub-element of personal information collected or to be collected necessary to administer the program or activity?

Statutory reference: Section 4 of *Privacy Act*

Policy reference: Sections 6.1.1, 6.1.3, 6.1.4, 6.2.7 and 6.2.8 of *Directive on Privacy Practices*

YES

- 2.1 ☒ Ensure that all personal information necessary to administer the program or activity is listed in

the relevant **PIB**.

****Personal Information Bank (PIB) should be found within "Section 1 – Overview and Initiation" above****

- 2.2 ☒ AND, implement controls and procedures to ensure the CBSA does not collect more personal information than is necessary for the identified program or activity and that a continuing need exists for that information or its collection.

****Ensure to provide the "controls and procedures" as an annex to this PIA** (Annex D)**

- 2.3 Are secondary uses contemplated for the information collected?

****Treasury Board defines a "Secondary Use" as a purpose that is not consistent with the original purpose of the collection.****

☐ YES ☒ NO (Continue to Question 3)

****If you've selected "Yes" to Question 2.3 above, please note that Consent is required for all "Secondary Uses". Please ensure that a "Consent Statement" is created. Please refer to "4. Direct Collection - Notification and Consent (as appropriate)" below for the information required in a "Consent Statement".****

- 2.3.2 If not, is there authority for the use or disclosure of the personal information?

****Please ensure that the Legal Authority identified above allows for all uses and disclosures of the personal information.****

☒ YES ☐ NO

→ Continue to Question 3

NO

- 2.4 ☐ Review the proposed elements and sub-elements of personal information outlined in "Section 3 – Analysis of Personal Information Elements" to identify those that are "necessary" and not merely useful. Document any changes.

3. Authority For the Collection, Use or Disclosure Of the Social Insurance Number

Is the collection of the Social Insurance Number (SIN) necessary to administer the program or activity?

Statutory reference: Section 4 of *Privacy Act*

Policy reference: Section 6.2.13 of *Policy on Privacy Protection* and sections 6.1.1 and 6.2 to 6.4 of *Directive on Social Insurance Number*

Also see "Guidance for Preparing Information-Sharing agreements Involving Personal Information" and "Taking Privacy into Account Before making Contracting Decisions"

YES

- 3.1 ☐ Collection of the SIN must be in compliance with the *Directive on Social Insurance Number* (please check all appropriate boxes below):

3.2 ☐ State legal authority for collecting the SIN:

OR, in the absence of a legal authority to collect the SIN:

3.3 ☐ Establish explicit authority through legislative amendment(s).3.4 ☐ Establish legal authority as outlined in the *Directive on Social Insurance Number*.

AND, if disclosure of the SIN by the CBSA is to occur on a routine or systematic basis

3.4.1 ☐ to another federal institution that is authorized to collect it, or to another level of government, establish an agreement or arrangement that includes specific provisions to limit the use of the SIN.3.4.2 ☐ to a contractor or other external service provider, establish a contract that includes specific provisions to limit the use of the SIN.3.5 ☐ AND, ensure that the relevant **PIB** for the program or activity states the authority under which the SIN is collected and the purpose for which it is used.

→ Continue to Question 4

NO

3.6 ☒ The SIN is not necessary and it will not be collected, used or disclosed to administer the program or activity.

→ Continue to Question 4

4. Direct Collection - Notification and Consent (as appropriate)

Is personal information collected directly from the individual to whom it relates?

Statutory reference: Sections 4 and 5 of *Privacy Act*

Policy reference: Sections 6.1.1, 6.2.6 and 6.2.9 to 6.2.13 of *Directive on Privacy Practices* and section 6.1.2 and 6.4.1 of *Directive on Social Insurance Number*

YES

4.1 ☒ A "Privacy Notice" (adapted for either verbal or written communications) must be provided to the individual at the time of collection and it must include the following elements:

a) The purpose and authority for the collection

b) Any uses or disclosures that are consistent with the original purpose.

c) Any uses or disclosures that are not related to the original purpose

(This element need only be included when additional uses or disclosures on a regular basis are contemplated at the time of collection for a purpose other than the original purpose or a consistent use, in which case a "Consent Statement" may need to be added to the "Privacy Notice" – see below for "Consent Statement" elements.)

d) Any legal or administrative consequences for refusing to provide the personal information

e) That the "individual to whom the information relates" has rights of access to, correction of and protection of personal information under the *Privacy Act*.

f) A reference to the **PIB** for the program or activity

(This element need only be included when the notice is to be given to the individual in writing.)

****For a copy of the CBSA Privacy Notice and Consent Statement template, contact the ATI and Privacy Division.****

g) Why the SIN is collected, how it will be used and the consequence of not providing it.

(This element need only be included when the SIN is being collected – refer to “3. Authority For the Collection, Use or Disclosure Of the Social Insurance Number” above.)

AND, add a “Consent Statement” to the “Privacy Notice” as appropriate, if the personal information is to be used or disclosed for a purpose other than the original purpose (**Secondary Use**) or a consistent use, or, to authorize indirect collection of personal information.

4.2 ☒ The “Consent Statement” must include the following elements:

a) The purpose of the consent and the specific personal information involved.

b) In the case of indirect collections, the sources that will be asked to provide the information. (This element need only be included when personal information is to be collected from another source e.g., person or organization with the consent of the individual)

c) Uses and disclosures that are not consistent with the original purpose of the collection and for which consent is being sought.

(This element need only be included when the individual’s consent is sought for a secondary use or disclosure that is not consistent with the original purpose for which the information is collected. To find out if the individual’s consent is necessary for such a use or disclosure, please consult the ATI and Privacy Division)

d) Any consequences that may result from withholding consent.

e) Any alternatives to providing consent

****For a copy of the CBSA Privacy Notice and Consent Statement template, contact the ATI and Privacy Division****

4.3 ☒ AND, implement controls and procedures to ensure that the CBSA keeps a record documenting whether or not an individual provided consent when it was sought, including a record documenting any withdrawal of consent when applicable.

****Ensure to provide the “controls and procedures” as an annex to this PIA** (Annex E)**

→ Continue to Question 5

NO

4.4 ☐ The personal information necessary for the program or activity is not collected directly from the individual. It is collected indirectly, for example, from another program within the CBSA, or from another institution, government or third party.

→ Continue to Question 5

5. Indirect Collection - Consent or Authority Under Sec. 10 of Privacy Regulations

Is personal information collected indirectly from another source with the informed consent of the

individual to whom it relates, or from a person authorized to act on behalf of the individual pursuant to section 10 of the Privacy Regulations?

Statutory reference: Sections 4 and 5 of *Privacy Act* and section 10 of *Privacy Regulations*

Policy reference: Sections 6.1.1, 6.2.6 and 6.2.9 to 6.2.13 of *Directive on Privacy Practices* and sections 6.1.2 and 6.4.1 of the *Directive on Social Insurance Number*

YES

- 5.1 ☒ The notice and consent requirements stated at Question 4 apply. Please provide the "**Privacy Notice**" and/or "**Consent Statement**" below:

Canada's Privacy Statement

The information you provide in your application, including supporting documentation and biometric data, is collected by the Canada Border Services Agency (CBSA) and is protected pursuant to both the *Customs Act* and the *Privacy Act*. In accordance with Canadian laws and regulations, this information will be shared with other government departments or agencies in Canada and the United States of America for the purpose of the operation of the NEXUS program and to conduct applicable checks and verifications to determine your eligibility and continued eligibility in the NEXUS program. If the required information is not provided, your application may not be processed and the authorization may not be granted.

Individuals to whom the information relates have rights of access to, correction of and protection of, their personal information under the *Privacy Act*. The information collected is described in Personal Information Bank # CBSA PPU 031. Instructions for obtaining information are provided in Info Source, which is available at public libraries, government public reading rooms and on the Internet at: <http://infosource.gc.ca>.

Consent Statement

I understand that any information gathered for the purposes of this application, including any supporting documentation, background information, biometric data and information obtained from the relevant files of law enforcement agencies, including intelligence gathered for law enforcement purposes, will be used for the purpose of the operation of the NEXUS program and to conduct applicable checks and verifications to determine eligibility and continued eligibility in the NEXUS program as described in the *Presentation of Persons (2003) Regulations*. My contact information may also be used by the CBSA to send me notifications related to changes to the NEXUS program.

In addition, I understand that my personal information gathered for the purposes of this application, including my supporting documentation, background information, biometric data, and any other information obtained and collected for the purpose of the operation of the NEXUS program and to conduct applicable checks and verifications to determine my eligibility and continued eligibility in the NEXUS program, may be accessed and used by the CBSA, as well as by other government departments or agencies in Canada (including the Royal Canadian Mounted Police and the Canadian Security Intelligence Service), in accordance with the *Privacy Act*.

In addition to the above-noted use by the CBSA and other Canadian government departments and agencies, I also understand that the CBSA will share its determination of my eligibility to the NEXUS

program, based on Canadian criteria, with the United States Department of Homeland Security ("DHS"). The DHS will, in turn, disclose to the CBSA its determination of my eligibility based on the American criteria.

If you do not consent to the above-noted collection, use and sharing of your personal information, your application cannot be processed and an authorization cannot be granted.

Do you consent to the above noted collection, use and sharing of your personal information AND do you certify that all the information given on this application, and in support of this application, is provided voluntarily and is true, accurate and complete, and that you have read, understood, and agree to abide by all conditions applicable to the program to which you apply and to the use of the associated authorization, including all instructions and notices accompanying this application? ☐ Yes ☐ No

- 5.2 ☒ AND, implement controls and procedures to ensure the CBSA keeps a record documenting whether or not an individual provided consent when it was sought, including a record documenting any withdrawal of consent when applicable.

****Ensure to provide the "controls and procedures" as an annex to this PIA** (Annex E)**

- 5.3 ☒ AND, if information is being collected from persons authorized to act on behalf of minors, incompetents or individuals who have been deceased for less than 20 years, implement appropriate mechanisms to ensure that such persons are authorized to act on behalf of individuals who do not have the capacity to provide consent.

****Ensure to provide the "mechanisms" as an annex to this PIA** (Annex E)**

Note: *With respect to minors, there is a standard mechanism in place to ensure the recognition of persons authorized to make decisions on behalf of others. The NEXUS application form states, "If applying for a child under 18 years of age, you must ensure that you provide documentary evidence that you have authority to apply on behalf of the child and that a photocopy of all legal documents regarding custody are submitted." In such circumstances the parent or guardian will present this documentary evidence to the CBSA and U.S. CBP officers during the interview at the EC. The NEXUS website (www.nexus.gc.ca) does provide information on using a third party representative to apply for the program.*

→ Continue to Question 6

NO

- 5.4 ☐ → Continue to Question 6

6. Indirect Collection - Without Notification and Consent

Is personal information collected from another source without notice to or consent from the individual to whom the information relates?

Statutory reference: Sections 4, 5, 7 and 8 of *Privacy Act* and section 10 of *Privacy Regulations*
Policy reference: Sections 6.2.6 and 6.2.9 to 6.2.13 of *Directive on Privacy Practices*, section 6.2.15 of the *Policy on Privacy Protection* and sections 6.3.2 and 6.3.3 of *Directive on Privacy Impact Assessment*

YES

6.1 ☐ Where information is collected indirectly under any of the following circumstances without notice to, or consent from, the individual to whom it relates, please check the applicable boxes and explain as requested:

- ☐ a) The collection is a result of a disclosure to the CBSA under subsection 8(2) of the *Privacy Act*. State the applicable paragraph(s) of subsection 8(2) and provide a brief explanation for each:

Details: (This information is mandatory)

- ☐ b) Direct notification of the individual might result in the collection of inaccurate information, or might defeat the purpose or prejudice the use for which the information is collected. Briefly explain why notice is not provided: (For example, certain kinds of lawful investigation might be jeopardized if the investigators were required to notify the individuals who were the subjects of the investigations before collecting information indirectly from other sources.)

Details: (This information is mandatory)

- ☐ c) The information involved in the program or activity is to be used solely for a non-administrative purpose in which no decisions are made about the individuals to whom the information relates. (This includes research, statistical, audit or evaluation purposes.)

6.2 ☐ AND, if any of the circumstances in a) b) or c) is applicable, ensure that it is reflected in the relevant **PIB**.

6.3 ☐ AND, if the information is to be used solely for a non-administrative purpose (box c above has been checked), ensure that the requirements under sections 6.3.2 and 6.3.3 of the *Directive on Privacy Impact Assessment* have been met, and that the decision of the official responsible for section 10 of the *Privacy Act* to proceed with a CBSA PIA for the program or activity has been adequately documented in the description of the program or activity in "Section 1 - Overview and PIA Initiation" of the CBSA PIA.

6.4 ☐ OR, if none of the circumstances in a) b) or c) is applicable, then the personal information must be collected directly from the individual, or indirectly with the consent of the individual. Please review the responses to Questions 4 and 5 and ensure that the "Privacy Notice" or the "Consent Statement" includes all of the required elements within Question 4.

→ Continue to Question 7

NO

6.5 ☒ All personal information is collected directly from the individual to whom it relates, or from another source with notice to, or consent from, the individual or a person authorized to act on behalf of the individual (see Questions 4 and 5 above). → Continue to Question 7

7. Retention and Disposal of Personal Information

Has Library and Archives Canada approved a records retention and disposal schedule that applies to the personal information? (Consult Information Management officials to determine the authority to

retain and dispose the personal information and provide the relevant details below.)

Note: Information Management has indicated that Library and Archives Canada does not approve retention and disposition schedules. That is an internal process that involves the OPI and IM Operations (ISTB-EAIM-EIMD-IM Operations). CBSA business determines and approves retention schedules.

The Information Management Unit must approve answers to this section.

Statutory reference: Section 12 of *Library and Archives Canada Act*, sections 6, 10 and 11 of *Privacy Act* and section 4 of *Privacy Regulations*

Policy reference: Sections 6.1.3, 6.2.11 to 6.2.13 and 6.2.23 of *Directive on Privacy Practices*

YES

- 7.1 ☒ Please identify the Record Disposition Authority (RDA) and describe the retention and disposal schedule: (For example, RDA Number: 79/002, records are retained for 10 years -- active for five and dormant for five. Destruction through agreement with Library and Archives Canada.)

Details: CBSA inherited RDA 2000/033 from the CRA and it was within the purview of the CBSA to apply the RDA during the time period ranging from 2003 to March 20, 2015. However, on March 31, 2015, Library and Archives Canada provided the CBSA with its first Disposition Authorization (DA). This institution-specific DA (2015/008) supersedes all authorities used in the past emanating from the CRA or IRCC. Acquiring a new RDA does not nullify the validity of any existing retention and disposition schedules under the previous RDA 2000/033, but they will now be enforced through DA 2015/008. At the end of the retention period, the business owner must complete the "Records Storage or Records Destruction" form and seek approval from the Director of the Office of Primary Interest and the Director of Information Management (IM) for disposition of the records. The IM Director will keep the signed forms for 10 years after the record(s) is destroyed as the disposition of information resources of business value must always be documented and approved before any action is taken.

- 7.2 ☒ AND, implement controls and procedures to ensure that personal information used to make a decision that directly affects an individual will be retained for a minimum of two years after the last administrative action or, where a request for access to the information has been received, until such time as the individual has had the opportunity to exercise all his/her rights under the Act. (For example, the information must be retained for at least two years after the CBSA ATI and Privacy Division responded to the request. If the requestor complains to the Privacy Commissioner, the information must be retained for at least two years following the Commissioner's finding on the complaint. If the finding is reviewed by the Federal Court, then the information must be retained for at least two years after that review is completed, and so on.)

****Ensure to provide the "controls and procedures" as an annex to this PIA** (Annex F)**

- 7.3 ☒ AND, if the CBSA intends to dispose of personal information that has been used for an administrative purpose prior to the expiration of the two-year minimum retention standard established by the *Privacy Regulations*, it must obtain the consent of the individual to whom the information relates before doing so. (This may occur if, for example, within the two year period it is determined that the information is incorrect and that the most appropriate means of correction is disposal, or if the information is no longer required. The consent of the

individual to dispose of the personal information must be obtained in writing.)

- 7.4 ☒ AND, the CBSA must cite the RDA number, the retention period and the disposition standards for the personal information in the relevant PIB.

→ Continue to Question 8

NO

- 7.5 ☐ Provide a Records Disposition Submission to Library and Archives Canada describing the records containing the personal information for which the institution requires a RDA.
- 7.6 ☐ AND, obtain a RDA from Library and Archives Canada to allow the CBSA, under certain conditions, to dispose of records that no longer have operational utility for the program or activity.
- 7.7 ☐ AND, ensure that all the other applicable requirements listed under "YES" at Question 7 are met.

→ Continue to Question 8

8. Accuracy Of Personal Information

Will measures be adopted to ensure that personal information used by the CBSA for an administrative purpose is as accurate, up-to-date and complete as possible?

Statutory reference: Sections 6, 10 and 11 of *Privacy Act* and sections 10 and 11 of *Privacy Regulations*

Policy reference: Sections 6.1.1 and 6.2.9 to 6.2.16 of *Directive on Privacy Practices*

YES

- 8.1 ☒ Please check any of the following measures that will be adopted to ensure accuracy of the personal information and provide details as requested:
- 8.1.1 ☒ Personal information will be collected directly from the individual to whom it relates or it will be validated with the individual or a person authorized to act on behalf of the individual.
- 8.1.2 ☒ A data-matching process will be used to verify the accuracy of personal information against a "reliable source" (within or outside the CBSA) where this is authorized, or where consent was obtained.

Details: Whether under the current system (paper-based applications or electronic applications through GOES) or through NEXUS eGate, data matching is used to eliminate inaccurate or duplicate information at enrolment and to risk assess applicants and to ensure that existing NEXUS members remain in good standing. This is consistent with the stated purpose of data collection i.e. the administration of NEXUS, and that this activity is disclosed to prospective applicants during the application/interview process. Further, for CATSA, when a NEXUS member uses the dedicated CATSA line, he/she uses the RFID embedded in the card that will prompt a picture of the member associated with that card on a screen for a security officer to view and match the person using the CATSA line. If the security officer deems it to be a match, the officer releases the gate to allow the member through; if it is not a match, the security officer does not release the gate and the person is sent back to the regular security screening line. Nothing more

than the person's photo is displayed to the security officer at the CATSA line. After the photo is viewed, the CATSA information system will delete the photograph.
(See also Schedule O – Data Matching – Online NEXUS Application)

- 8.1.3 ☐ In cases where direct collection or consent is not feasible, the CBSA will obtain information from trusted sources (public or private) and verify accuracy against existing personal information before use.

Details: Identify the sources and procedures to be used to check the accuracy of the information

- 8.1.4 ☒ Technological methods will be used to identify errors and discrepancies.

Details: Data matching is used to eliminate inaccurate or duplicate information at enrolment and to risk assess applicants and to ensure that existing NEXUS members remain in good standing. This is consistent with the stated purpose of data collection i.e. the administration of NEXUS. This activity is disclosed to prospective applicants during the application/interview process. It is also used for CATSA screening and NEXUS eGate (see s. 8.1.2 above).

- 8.1.5 ☐ Other

Specify: (This information is mandatory)

- 8.2 ☒ AND, if measures are adopted other than "direct collection or validation with the individual or with a person authorized to act on behalf of the individual", the CBSA must implement appropriate controls and procedures to ensure that:
- a) the technique(s) and the specific source(s) used to validate or update the personal information are documented;
 - b) individuals are given the opportunity, whenever possible, to request correction of any inaccurate personal information before the information is used in a decision-making process that affects them;
 - c) personal information can only be modified or corrected by those within the CBSA who have the authority to do so;
 - d) when personal information is corrected or annotated, the record of personal information indicates the date of the last correction or annotation and the source of the information used to make the correction or annotation; and
 - d) when personal information is corrected or annotated, other authorized holders of the information are notified about the correction or annotation and that all copies of the information in the possession of the CBSA are corrected / annotated.
- 8.3 ☒ AND, if appropriate, ensure that the "Privacy Notice" or "Consent Statement" and the relevant **PIB** are amended to identify the data-matching activity including the source(s).

→ Continue to Question 9

NO

- 8.4 ☐

Explain why such measures will not be adopted: (This information is mandatory)

→ Continue to next Question 9

****Ensure to provide all relevant "controls and procedures" implemented as a result of the above requirements as an annex to this PIA** (Annex G)**

9. Use Of Personal Information

Will the personal information collected for the program or activity be used solely for the original purpose for which it was obtained or compiled, a use consistent with that purpose, or a purpose for which the information was disclosed to the institution pursuant to subsection 8(2) of the Privacy Act?

Statutory reference: Sections 5 and 7 to 11 of *Privacy Act*

Policy reference: Sections 6.1.1, 6.1.9, 6.2.9 to 6.2.13 and 6.2.17 of *Directive on Privacy Practices*, section 6.2.15 of *Policy on Privacy Protection* and Section IV of Appendix C of *Directive on Privacy Impact Assessment*

YES

- 9.1 ☒ Implement controls and procedures to ensure that access to the personal information for such purposes will be limited to authorized individuals who need to know the information to perform their official duties. *(Identify the work positions within the program or activity that have a valid reason to access and handle the personal information, and limit access to individuals occupying those positions.)* See Section 4.6 (Other Possible Considerations)
- 9.2 ☒ AND, ensure that the "Data Flow Diagram" or "Data Flow Tables" completed for "Section 4 – Flow of Personal Information" of the CBSA PIA identify the areas, groups and individuals (e.g., the positions) within the CBSA who have a need-to-know to access to or handle the personal information, including their geographical location and where the personal information will be stored or retained. *(See Section IV of Appendix "C" of Directive on Privacy Impact Assessment for a list of elements that must be included in the data flow diagram or data flow tables.)*
- 9.3 ☒ AND, if the purposes for which the personal information is used includes any use(s) of the information for a non-administrative purpose, (such as research, statistical, audit and evaluation purposes) the CBSA will adhere to the requirements and principles in the **CBSA Privacy Protocol For Non-Administrative Purposes** (2012), in accordance with section 6.2.15 of the *Policy on Privacy Protection*, to address any impact that such non-administrative uses may have on privacy.

→ Continue to Question 10

- 9.4 ☒ AND, ensure the use of personal information is compliant with CBSA's Privacy Code of Ethics.

Note: Personal information data will be used for the purposes for which the CBSA originally collected the data, that is, to make a determination on the applicant for membership eligibility either during initial enrolment or at membership renewal as well as for the administration of the individual's membership record during the period of their participation in the program. For example, personal information is used to compare transitory iris images captured at passage in the air mode to establish a match for identity purposes. Disclosure of information for other reasons is only

undertaken pursuant to section 107 of the *Customs Act* and in accordance with the CBSA Policy on the Disclosure of Customs Information (see Schedule H). Biometric information captured during enrolment (e.g. iris scan), is used to identify the member during air passage. Individuals are not required to provide their iris biometric if they do not intend to travel by air.

****Ensure to provide the "controls and procedures" as an annex to this PIA** (Annex H)**

NO

- 9.5 ☐ Identify below any other uses of the personal information, in other words, any routine uses that are not directly related to the purpose of the collection, or, which are not consistent with that purpose or for which the information was disclosed to the CBSA pursuant to subsection 8(2) of the *Privacy Act*:

Detail : (This information is mandatory)

- 9.6 ☐ AND, ensure that these other uses are reflected in the relevant **PIB**. (In accordance with subsection 9(1) of the *Privacy Act*, if these other uses are not described in the PIB in CBSA Info Source, the CBSA is required to record each use on the individual's file. Describing them in the PIB is, therefore, a far more efficient practice – see Question 11.)
- 9.7 ☐ AND, include a description of these other uses in the "**Privacy Notice**" or "**Consent Statement**", as appropriate,
- ☐ AND, ensure the all the other applicable requirements listed under "**YES**" at Question 9 are met.

→ Continue to Question 10

10. Disclosures Directly Related to the Administration of the Program or Activity

Will personal information be disclosed for purposes directly related to the administration of the program or activity? (This includes, for example, disclosures to other programs within the CBSA, other federal institutions, other governments, international organizations, private sector organizations or individuals.)

If there are new or modified MOUs or ISAs as part of the program, the IMU must be consulted and the IMU must approve/endorse the responses to this question.

Statutory reference: Sections 5 and 8 to 11 of *Privacy Act*.

Policy reference: Sections 6.2.10, 6.2.11 and 6.2.13 of *Policy on Privacy Protection*, sections 6.2.1 to 6.2.3 of *Directive on Social Insurance Number*, sections 6.1.9, 6.2.9 to 6.2.13 and 6.2.15 to 6.2.20 of *Directive on Privacy Practices* and section IV of Appendix "C" of *Directive on Privacy Impact Assessment*)

Also see "Guidance for Preparing Information-Sharing agreements Involving Personal Information" and "Taking Privacy into Account Before making Contracting Decisions"

YES

- 10.1 ☒ Please check all applicable boxes below and, for each disclosure, identify the name of the

organization or third party to which personal information will be disclosed. If it is disclosed within the CBSA, please identify the branch and the program or activity.

- 10.1.1 ☒ Within the CBSA for another program or activity

Details: Operations Branch (BSOs at any of Canada's eight international airports and Billy Bishop Toronto City Airport and at NEXUS land ports of entry); Recourse Directorate (Appeals Analyst); Program & Policy Management Division (Senior Program Advisor, Senior Program Officer, Manager); Business Systems Integration Division (Manager, Senior Program Advisor, Senior Program Officer); and, Stakeholder Engagement and Outreach unit (Senior Program Advisors, Senior Program Officers, Junior Program Officers). See section 4.6 above.

- 10.1.2 ☒ Other federal government institutions

Details: IRCC; RCMP; CATSA

- 10.1.3 ☐ Provincial, territorial or municipal governments institutions

Detail : *(This information is mandatory)*

- 10.1.4 ☒ Foreign government institutions and entities thereof

Details: U.S. CBP (see MoU at Schedule A), and GPO

- 10.1.5 ☐ International organizations

Detail : *(This information is mandatory)*

- 10.1.6 ☐ The private sector (e.g., contractor or other external service provider)

Detail : *(This information is mandatory)*

- 10.1.7 ☐ Other

Detail :

- 10.2 ☒ AND, ensure that:

- a) any such disclosure is made in compliance with section 8 of the *Privacy Act*, which allows disclosures of personal information with consent of the individual to whom the information relates (subsection 8(1)) or without consent in certain and limited circumstances pursuant to subsection 8(2) of the Act;
- b) only personal information elements that are necessary for the intended purpose are disclosed;
- c) the organization or third party receiving the personal information is authorized to do so;
- d) administrative, physical and technical safeguards appropriate to the sensitivity of the information will be applied to protect the information during and after its transmission (see

Question 15);

- e) the organization or third party to which the personal information will be disclosed for the administration of the program or activity are identified in the "Consistent Use" section in the relevant **PIB** in *CBSA Info Source*, including the specific purpose of the disclosure; the "Privacy Notice" or "Consent Statement" describes any disclosures of information; (For a copy of the CBSA Privacy Notice and Consent Statement template, contact the ATI and Privacy Division) and,
- f) the "Data Flow Diagram" or "Data Flow Tables" completed in "Section 4 – Flow of Personal Information" of the CBSA PIA include details on the disclosed personal information: (See Section IV of Appendix "C" of *Directive on Privacy Impact Assessment* for a list of elements that must be included in the data flow diagram or data flow tables.)

10.3 ☒ AND, any disclosure of personal information to another federal institution or outside the Government of Canada is governed by a formal agreement or arrangement (e.g., a Memorandum of Understanding, an accord, a contractual arrangement, etc.) to ensure that appropriate privacy protection clauses are included, and, where applicable, include provisions for inter-jurisdictional or transborder flows of personal information. Such clauses must cover the following topics:

- a) Control over personal information, where appropriate.
- b) Limitations on the collection, retention, use and disclosure of personal information.
- c) Measures (administrative, technical and physical) to protect the integrity and confidentiality of personal information.
- d) Measures governing the disposition of the personal information, where relevant
- e) Measures to ensure or verify that the personal information is only used for the purposes related to the agreement, arrangement or contract.
- f) Obligations are to be extended to other parties such as subcontractors.

→ Continue to Question 11

NO

10.4 ☐ There is no disclosure of personal information within or outside the institution for purposes that are directly related to the administration of the program or activity.

→ Continue to Question 11

11. Accounting For New Uses or Disclosures Not Reported in CBSA Info Source

Will controls and procedures be implemented to account for any new use or disclosure of the personal information that is not included in the relevant **PIB** published in CBSA Info Source?

Statutory reference: Sections 7 to 11 of *Privacy Act* and section 4 of *Privacy Regulations*

Policy reference: Sections 6.1.9 and 6.2.2 of *Directive on Privacy Practices*

YES

11.1 ☒ Appropriate controls and procedures have been or will be implemented to ensure that:

- a) the head of the institution (The ATI and Privacy Director) or the appropriate delegate is notified about any new use or disclosure of personal information that is not reflected in the PIB description published in *CBSA Info Source*;
- b) the consent of the individual to whom the information relates is obtained in writing, as appropriate, prior to any new use of the information for an administrative purpose that is not reflected in the relevant PIB published in *CBSA Info Source*, unless the new use is considered to be consistent with the purpose for which the personal information was obtained or compiled and the Privacy Commissioner is notified, by the CBSA ATI and Privacy Director, forthwith regarding the new consistent use;
- c) except as permitted under subsection 8(2) of the *Privacy Act*, any disclosure of personal information for a purpose that is not reflected in the relevant PIB published in *CBSA Info Source* will only be made with the consent of the individual to whom the information relates;
- d) a record is kept for any new use or disclosure of personal information not described in the relevant PIB published in *CBSA Info Source*, and that this record is stored with the personal information to which it relates and retained for a minimum period of two years following such a use or disclosure; *(The record of use or disclosure should include the name and title of the person authorizing the use or disclosure; the name of the institution, person, organization or body receiving the information; a description of the use or purpose of disclosure; a copy of the information disclosed, or a description in sufficient detail to allow a determination of exactly what information was used or disclosed.)*
- e) if the information is disclosed to a federal investigative body under paragraph 8(2)(e) of the *Privacy Act*, the record of disclosure will be kept in a separate PIB for a period of two years where it will be available to the Privacy Commissioner for review upon request; *(e.g., Standard PIB "Disclosure to Investigative Bodies" PSE 913)*
- f) the Privacy Commissioner is notified, by the CBSA ATI and Privacy Director, forthwith, as required under subsection 9(4) of the Act, of any new use or disclosure that is consistent with the purpose for which the information was obtained or compiled, but which is not reflected in the relevant PIB published in *CBSA Info Source*;
- g) the relevant PIB is amended in time for the next edition of *CBSA Info Source* to include any new use(s) or disclosure(s) that are consistent with the purpose for which the information was obtained or compiled, as well as any routine use(s) or disclosure(s) that do not fall within the categories of purpose of collection or consistent use (e.g., these would include disclosures of the information under subsection 8(2) of the Act that take place on a regular basis. By including these routine uses or disclosures in the PIB, the CBSA would be relieved from the obligation to record each use or disclosure on the individual's file); and
- h) the Privacy Commissioner is notified, by the ATI and Privacy Director, prior to or forthwith, as required under subsection 8(5) of the Act, about any disclosures made or to be made in the public interest or in the interest of the individual to whom the information relates.
- i) Other

Details: The NEXUS program does not disclose personal information to law enforcement agencies during the risk assessment process, with one exception. NEXUS information is considered "customs information" as defined by the *Customs Act* and can be used or shared in accordance with section 107 of the *Customs Act* and in accordance with the CBSA Policy

on the Disclosure of Customs Information (see Schedule H); both of which provide strict, limited, and specific circumstances where such information may be shared (i.e. defense of Canada, public safety, or law enforcement). As an example, the CBSA may disclose address information to the RCMP where a warrant for arrest exists against an applicant. This disclosure is authorized by the Chief of Intelligence and a record of the release of information is maintained.

→ Continue to Question 12

NO

- 11.2 ☐ Please explain why such controls and procedures will not be implemented

Detail: Provide adequate justification.

→ Continue to Question 12

12. Safeguards - Statement Of Sensitivity

Has a Statement of Sensitivity (SoS) or similar analysis been completed to assess the degree of sensitivity of the personal information to be collected and retained for the program or activity? (Input to this section should be coordinated with and reviewed by the CBSA – IT - Security Directorate)

Statutory reference: Sections 7 and 8 of Privacy Act.

Policy reference: Appendix C of *Directive on Privacy Impact Assessment* and sections 6.2.17 to 6.2.21 of *Directive on Privacy Practices, Policy on Government Security, Operational Security Standard: Management of Information Technology Security (MITS)*

YES

- 12.1 ☒ The information contained in the SoS or similar analysis has been taken into account when assessing the level of risks to privacy in "Section 2 - Risk Area Identification and Categorization" of the CBSA PIA.

Note: An SoS has been completed for GEC (Schedule R), the Trusted Traveller Programs (Schedule V), Passage – NEXUS Air Pilot Project (Schedule W), NEXUS Highway Passage (Schedule DD), NEXUS Highway Application SoS (Schedule EE), NEXUS Airport Kiosk – Passage (Schedule RR) and CATSA (Schedule VV). No significant risks were identified in the above mentioned SoS processes. Minor risks have or will be addressed through Standard Operating Procedures changes or technology advancements.

→ Continue to Question 13

****A SoS is not necessarily required as an Annex to this PIA. CBSA's IT Security Directorate must approve of the SoS being attached as an Annex, which also includes the review and approval of any SoS excerpts. ****

NO

- 12.2 ☐ Please explain why a SoS or similar analysis was not considered necessary to assess the

sensitivity of the information.

Detail : (This information is mandatory)

→ Continue to Question 13

13. Safeguards - Threat and Risk Assessment

Has a Threat and Risk Assessment (TRA) or a similar security assessment been completed for the program or activity? (Input to this section must be coordinated with and reviewed by CBSA – IT - Security Directorate)

Statutory reference: Sections 7 and 8 of Privacy Act.

Policy reference: Appendix C of Directive on Privacy Impact Assessment and sections 6.2.17 to 6.2.21 of Directive on Privacy Practices, Policy on Government Security, Operational Security Standard: Management of Information Technology Security (MITS)

YES

- 13.1 ☒ Reference the title of the TRA or other security assessment in "Section 7 – Supplementary Documents List" and provide a brief synopsis of the assessment in the space below:

****Providing a summary of the TRA or annexing the TRA, or excerpts thereof, must not be done without the approval of IT Security.**

Details: A TRA has been completed for GEC (Schedule R), Trusted Traveller Programs (Schedule V), Passage – NEXUS Air Pilot Project (Schedule W), NEXUS Highway Passage (Schedule DD), NEXUS Highway Passage TRA (Schedule FF), and NEXUS Airport Kiosk - Passage (Schedule RR). No significant risks were identified in the above mentioned TRA processes. Minor risks have or will be addressed through Standard Operating Procedures changes or technology advancements.

TRA's for the NEXUS program, the RFID Processor which will allow the CBSA to read RFID-enabled documents including NEXUS cards, and for the usage of RFID technology, have not been completed. To address this, the CBSA is in the process of completing a TRA to address these issues. The completion dates are not yet known, however, the process has been started.

- 13.2 ☐ AND, obtain assurances from the officials responsible for the program or activity that the measures recommended in the assessment have been implemented to ensure the confidentiality, availability and integrity of the personal information.
- 13.3 ☐ AND, ensure that any residual risks to personal information are known and accepted by the executive or senior official responsible for the program or activity and the Head or delegated authority for the Privacy Act. (ATI and Privacy Director)

→ Continue to Question 14

NO

- 13.4 ☐ If a TRA or similar security assessment is underway, simply reference that fact in the space below and indicate when it is likely to be completed. If there is no intent to complete one,

please explain.

Detail : (This information is mandatory)

→ Continue to Question 14

14. Safeguards - Administrative, Physical and Technical

Please identify below any administrative, physical and technical safeguards in place, or to be implemented, for this program or activity to ensure the confidentiality, availability and integrity of the personal information. (Safeguards must be commensurate with the sensitivity of the information, the risks identified, and the nature of the media in which the information is stored, handled and transmitted. This section must be completed with input from CBSA – IT - Security Directorate)

Statutory reference: Sections 7 and 8 of Privacy Act

Policy reference: Appendix C of Directive on Privacy Impact Assessment and sections 6.2.17 to 6.2.21 of Directive on Privacy Practices, Policy on Government Security, Operational Security Standard: Management of Information Technology Security (MITS)

Please also see Annex H – Controls and Procedures Implemented to Limit Access to Personal Information

Please check all that apply, including safeguards identified by the TRA or similar security assessment.

14.1 Administrative safeguards

- ☒ Internal security and privacy policies and procedures
- ☒ Staff training on privacy and the protection of personal information
- ☒ Screening and security checks of employees
- ☒ Appropriate security levels for employees who will have access to personal information
- ☐ Contingency plans and documented procedures in place to identify and respond to security and privacy breaches, and to communicate security violations to the data subject, law enforcement authorities and relevant program managers
- ☐ Regular monitoring of users' security practices
- ☐ Methods to ensure that only authorized personnel who need to know have access to personal information
- ☐ Other

Details: For GEC, all personnel are security cleared to the highest level of sensitivity of data processed; there are also established security policies, standards and procedures in place.

14.2 Physical safeguards

- ☒ Restricted access areas
- ☒ Security guards
- ☒ Identification badges are worn by staff at all times

- ☐ After hours alarms and monitoring systems
- ☒ Locked filing cabinets
- ☐ Combination locks
- ☐ Safes
- ☐ Cipher locks
- ☐ Key cards
- ☐ Video surveillance (closed-circuit television)
- ☒ Secured server locations
- ☐ Backups secured off-site
- ☒ Other

Details: GEC resides on a mainframe in a secure (restricted) area and uses virus scans, network ID and passwords for access.

For the NEXUS kiosks it has been determined that because the kiosk that houses the hardware resides in the Custom's Hall, deemed to be a secure area, no additional physical security requirements are required. However, the kiosks are secured to the floor and are constructed of steel casing with secure locks (as specified by the kiosk Request For Proposals).

14.3 Technical safeguards

- ☐ Role-based user authorization and authentication
- ☐ Biometrics
- ☒ Passwords (minimum of 6 characters long, include alpha and numeric characters)
- ☐ Passwords are changed by users every 90 days and recently used passwords cannot be re-used)
- ☐ Password protected screensavers
- ☒ Session-time out security (automatically locks an account after a session has been idle for a specified amount of time)
- ☒ Firewalls
- ☐ Intrusion Detection System (IDS)
- ☐ Virtual Private Network (VPN)
- ☒ Encryption of sensitive information
- ☐ Government of Canada Public Key Infrastructure Certificates (PKI)
- ☐ External Certificate Authority (CA)
- ☒ Audit trails
- ☐ Other

Details: GEC uses passwords to access data and User Audits.

NEXUS kiosks use audit trails to ensure a user's actions can be traced back to that individual; various databases are accessed for query during a passage including Global Enrolment, RAC, ICES and GCMS. All database writes or modifications log the user's

name and timestamp. A kiosk-specific audit log is also created during the time of passage.

An activity log is also maintained for all transactions made on an individual's membership record.

Each time that NEXUS membership is modified in ICS, an audit trail is established that tracks user identification, date modified and field(s) modified. An audit trail is not recorded when data is merely accessed for review purposes; privacy risks of an unauthorized person accessing the system are minimized through security and training given to authorized ICS users. Compliance reviews are not currently being done to determine if authorized ICS users are accessing NEXUS membership information. Nevertheless, with the safeguards in place, the risk of compliance being abused or misused is considered minimal.

User activity of GEC and the CPCS within the CBSA can be monitored since the user making the modifications to data and the date and time of the modification are logged. Firewalls are used to protect the integrity of the data storage. Once information is modified by either the CBSA or the U.S. CBP, this information will be updated to other agencies' internal systems.

Procedures and technical solutions are also in place to protect the system/application/data from being accidentally or deliberately disclosed or compromised including: segregation of tasks; ICS User profiles in use; secured work environment; Enhanced reliability security level for all staff; secured data link for purposes of transferring data between CBSA and U.S. CBP.

There is also a log of CATSA use.

→ Continue to Question 15

****Ensure to provide the "controls and procedures" as an annex to this PIA****

15. Technology and Privacy - Tracking Technologies

Will the information system(s) used to deliver the program or activity employ cookies or other tracking technologies to collect personal information about users and their transactions? (Input to this section should be coordinated with and reviewed by the CBSA – IT - Security Directorate)

Statutory reference: Sections 4 to 10 of the Privacy Act and section 4 of Privacy Regulations

Policy reference: Subsections 6.1.1, 6.1.3, 6.1.9, 6.2.9 to 6.2.13, 6.2.17 and 6.2.23 of Directive on Privacy Practices

YES

- 15.1 ☒ The specific tracking technologies to be used is adequately described under Part 6: Technology and Privacy of "Section 2 – Risk Area Identification and Categorization" of the CBSA PIA; (For example, the use of an audit trail that records information, such as user logon ID, date and time

of logon, logout, user location, terminal identity, name and ID of client records accessed, including edits or changes made during each user session, etc. The information is used to verify that only authorized users access personal information and to ensure that access can be linked to specific individuals to support the investigation of suspected or alleged misuse. The information is retained for a period of two years.)

- 15.2 ☒ AND, the collection of any personal information using such technologies is reflected in the relevant **PIB** and in "Section 3 – Analysis of Personal Information Elements" of the CBSA PIA;
- 15.3 ☒ AND, the use of such technologies to collect information about users and their transactions is adequately reflected in the "Privacy Notice";
- 15.4 ☒ AND, those responsible for implementing and using tracking technologies to collect personal information or who may have access to personal information collected through these methods are made aware of privacy and security policy requirements;
- 15.5 ☒ AND, where personal information collected through such tracking technologies is used to make a decision that directly affects the individual to whom the information relates, it will be retained for a minimum of two years after the last administrative action as required under the *Privacy Regulations*.

→ Continue to Question 16

NO

- 15.6 ☐ Tracking technologies are not used to collect personal information about users.

→ Continue to Question 16

16. Technology and Privacy - Surveillance or Monitoring

Will the new or modified program or activity result in new or increased surveillance or monitoring of a targeted population? (Input to this section should be coordinated with and reviewed by the CBSA – IT - Security Directorate)

Statutory reference: Sections 4 to 10 of *Privacy Act*, section 4 of *Privacy Regulations* and section 8 of the *Charter of Rights and Freedoms*

Policy reference: Subsections 6.1.1, 6.1.9, 6.2.9 to 6.2.13 and 6.2.17 of *Directive on Privacy Practices*

YES

- 16.1 ☐ Consult with your legal advisors to determine whether or not such surveillance or monitoring activities raise any issues relating to the *Charter of Rights and Freedoms*, the *Privacy Act* or other applicable acts.
- 16.2 ☒ And, ensure the surveillance or monitoring method(s) to be used, the characteristic(s) of the targeted population and the scope of the surveillance or monitoring are adequately described under Part 6: Technology and Privacy of "Section 2 – Risk Area Identification and Categorization" of the CBSA PIA.
- 16.3 ☒ AND, any personal information collected or created as a result of such surveillance or monitoring is described in the relevant **PIB** and in *Section 3 – Analysis of Personal Information Elements* of the CBSA PIA.
- 16.4 ☒ AND, the collection or use of personal information through surveillance or monitoring is adequately reflected in the "Privacy Notice", unless such notification might result in the

collection of inaccurate information or defeat the purpose or prejudice the use for which the personal information is collected.

☐ If notice about surveillance or monitoring will not be provided

Details: As a result of a pilot project at the Peace Bridge land border POE at Fort Erie, Ontario, called NEXUS eGate, 24/7 access is available at this NEXUS lane. NEXUS eGate remains functional at the POE pending the results of the analysis and a decision for a way forward. NEXUS eGate consists of two electronic gates (entrance and exit) installed in the NEXUS lane, a sensor to read the NEXUS card, video surveillance equipment to transmit images to the office and an intercom for the CBSA BSO to communicate with members in the vehicle. A BSO has the ability to access the CBSA system and view the NEXUS membership information and photo from within the CBSA office (using existing NEXUS technology). The capturing and storing of video transmission is the only aspect that is new to the NEXUS program. Video will be captured, stored and disposed of as per the Policy on the Overt Use of Audio-Video Monitoring and Recording Technology (attached at Schedule LL). There is no requirement to store audio transmissions/communications with this proof of concept.

The RFID initiative will:

- Allow faster secure capture of individual traveller information while in PIL prior to their arrival at the primary inspection booth;
- Allow effective risk assessment through automated queries, allowing BSOs more dedicated attention to traveller interviews where warranted; and,
- Increase public awareness of RFID-enabled documents and availability of RFID technology at Canada's border to facilitate and expedite border-crossing

16.5 ☒ AND, those responsible for implementing and using such surveillance or monitoring method(s) or who may have access to personal information collected or created through these methods are made aware of privacy and security policy requirements.

→ Continue to Question 17

NO

16.6 ☐ The new or modified program or activity will not result in surveillance or monitoring.

→ Continue to Question 17

17. Considerations Related to Compliance, Regulatory Investigation, Enforcement

Does the program or activity involve compliance/regulatory investigation or law enforcement, surveillance or intelligence gathering that targets specific individuals against whom penalties, criminal charges or sanctions may be applicable?

Statutory reference: Sections 4 to 10 of *Privacy Act*, section 4 of *Privacy Regulations* and section 8 of the *Charter of Rights and Freedoms*

Policy reference: Subsections 6.1.1, 6.1.9, 6.2.9 to 6.2.13 and 6.2.17 of *Directive on Privacy Practices*

YES

- 17.1 ☐ Consult with your legal advisors to determine whether or not the compliance/regulatory investigation or law enforcement activities raise any issues relating to the *Charter of Rights and Freedoms*, the *Privacy Act* or other applicable acts.
- 17.2 ☐ AND, identify the legislative authority and the specific regulatory or law enforcement purpose involved:

Detail: *(This information is mandatory)*

- 17.3 ☐ AND, if the legislative authority differs from the legal authority for the program or activity, ensure it is adequately reflected in the response to Question 1 of "Section 5 – Privacy Compliance Analysis" and in "Section 1 – Overview and PIA Initiation" of the CBSA PIA.
- 17.4 ☐ AND, any personal information collected or created as a result of such regulatory or criminal enforcement, surveillance or intelligence gathering program or activity is described in the relevant **PIB** and in "Section 3 – Analysis of Personal Information Elements" of the CBSA PIA.
- 17.5 ☐ AND, the collection or use of personal information through these compliance / regulatory investigation or enforcement activities is adequately reflected in the "**Privacy Notice**", unless such notification might result in the collection of inaccurate information or defeat the purpose, or prejudice the use, for which the personal information is collected.
- ☐ If notice about the compliance/regulatory investigation or law enforcement activities will not be provided.

Details explain why: *(This information is mandatory)*

NO

- 17.6 ☒ The program or activity does not involve the conduct of regulatory or criminal enforcement, surveillance or intelligence gathering.

SECTION 6 - Summary of Analysis and Recommendations

The ATI and Privacy Division will document the recommendations resulting from the risk identification and categorization, as well as in a manner that is commensurate with the risk identified. The risks and recommendations will be incorporated into the action plan as described in Annex B: Office of the Privacy Commissioner Expectations (2011)

Document the conclusion drawn or recommendations resulting from the risk identification and categorization in a manner that is commensurate with the risk identified.

ACCOUNTABILITY

Risks and Mitigations Strategies

Risk #1: A client may have concerns about the collection, use, disclosure or retention of their personal information.

Mitigation: The application process for NEXUS includes a clearly-designated requirement to provide consent for the use of any personal information collected, and indicates how the personal information will be used. All applicants must sign the application form, or fill out a field in the online application system to indicate that they understand and consent to the use of their information. Applicants under the age of 18 are required to have their parent or guardian complete the application and give consent on their behalf. Persons who are incapacitated will similarly have their authorised representative give consent on their behalf. Services are provided in both official languages at all enrolment facilities and information translation services for other major languages are also available at some ECs. All NEXUS applicants are subject to a face-to-face interview with a BSO. This interview provides an opportunity for the officer to evaluate the capacity of the individual to give consent to the collection of their personal information. If they are unable to provide consent it will be obtained from the power of attorney holder. Membership in the program is entirely voluntary, but consent to use personal information for program purposes is mandatory for membership. Applicants who refuse to provide consent to the use of their personal information will not be admitted into the program. Their application will not be processed, and no personal information will be retained.

If a client has a concern about the collection, use, disclosure or retention of their personal information, they may issue a complaint to the CBSA ATIP Division. They will be asked to include a brief description of the concern.

If a client is denied membership in the NEXUS program or are cancelled or suspended from the program by the CBSA, he/she may write to the Recourse Directorate at Headquarters or on-line within 90 days of the date shown on the NEXUS denial/cancelled/suspended letter, to request a review of the decision.

Recommendation: No further recommendations have been made

IDENTIFYING PURPOSES

Risks and Mitigations Strategies

Risk #2: A description of the NEXUS program and why each piece of information is collected may not be clear to the client.

Mitigation: NEXUS allows for customs and immigration border clearance processes to be streamlined for pre-approved, low-risk travellers, thus permitting the CBSA's resources to be allocated more effectively at the border. Membership is five years and provides expedited border clearance into Canada and the U.S. in the land, air and marine travel modes. NEXUS members use dedicated lanes in the highway mode; self-serve kiosks in the air mode; and, by reporting through TRC's in the marine mode. A full description of the NEXUS program is available at www.NEXUS.gc.ca.

To become a member of the NEXUS program, an applicant voluntarily submits an application using either a paper form sent to the CBSA or by applying electronically using the GOES maintained by the U.S.

CBP. When a paper application form is used, a clerk enters the information into GEC of the Integrated Customs System and it is assessed against a variety of enforcement databases to determine program eligibility. The personal information voluntarily provided by the applicant is used by the CBSA and CBP to confirm their identity and to determine the eligibility of an applicant and the continued eligibility of a member through a risk assessment.

The following personal information elements are managed by the NEXUS program and used to determine eligibility and continued eligibility in the program:

- full name
- contact information
- signature
- biographical information
- biometric information (for air travel only)
- citizenship status
- criminal checks/history
- date of birth
- credit card information (if not paying by certified cheque or money order); and
- identification numbers such as those contained on the birth certificate, driver's license or passport.

The NEXUS program is authorized under subsection 11.1(1) of the *Customs Act* and is also governed by the *Presentation of Persons (2003) Regulations*.

The NEXUS application form identifies the purpose for the collection and on-line notices of use. The form can be seen at the following link: <http://www.cbsa-asfc.gc.ca/prog/nexus/application-demande-eng.html>

The new NEXUS PIB is available at Schedule B.

Recommendation: No further recommendations have been made

CONSENT

Risks and Mitigations Strategies

Risk #3: Consent to use an individual's personal information might not be properly obtained from an individual. The collection and use of personal information generally requires the consent of the individual to whom the information pertains. There is a minimal risk that consent to collect information might not be obtained, either through a deficiency in the collection process, or because the individual was not able to give consent due to language barriers, age, incapacity, etc.

Mitigation: The personal information voluntarily provided by the applicant is used by the CBSA and CBP to confirm their identity and to determine the eligibility of an applicant and the continued eligibility of a member through a risk assessment.

The application process for NEXUS includes a clearly-designated requirement to provide consent for the use of any personal information collected, and indicates how the personal information will be used. All applicants must sign the application form, or fill out a field in the online application system to indicate that they understand and consent to the use of their information. Applicants under the age of 18 are required to have their parent or guardian complete the application and give consent on their behalf. Persons who are incapacitated will similarly have their authorised representative give consent on their behalf. Services are provided in both official languages at all enrolment facilities and information translation services for other major languages are also available at some ECs. All NEXUS applicants are subject to a face-to-face interview with a BSO. This interview provides an opportunity for the officer to evaluate the capacity of the individual to give consent to the collection of their personal information. If they are unable to provide consent it will be obtained from the power of attorney holder. Membership in the program is entirely voluntary, but consent to use personal information for program purposes is mandatory for membership. Applicants who refuse to provide consent to the use of their personal information will not be admitted into the program. Their application will not be processed, and no personal information will be retained.

Canada's revised Privacy & Consent Statement is as follows:

The information you provide in your application, including supporting documentation and biometric data, is collected by the Canada Border Services Agency (CBSA) and is protected pursuant to both the *Customs Act* and the *Privacy Act*. In accordance with Canadian laws and regulations, this information will be shared with other government departments or agencies in Canada and the United States of America for the purpose of the operation of the NEXUS program and to conduct applicable checks and verifications to determine your eligibility and continued eligibility in the NEXUS program. If the required information is not provided, your application may not be processed and the authorization may not be granted.

Individuals to whom the information relates have rights of access to, correction of and protection of, their personal information under the *Privacy Act*. The information collected is described in Personal Information Bank # CBSA PPU 031. Instructions for obtaining information are provided in Info Source, which is available at public libraries, government public reading rooms and on the Internet at: <http://infosource.gc.ca>

Consent Statement

I understand that any information gathered for the purposes of this application, including any supporting documentation, background information, biometric data and information obtained from the relevant files of law enforcement agencies, including intelligence gathered for law enforcement purposes, will be used for the purpose of the operation of the NEXUS program and to conduct applicable checks and verifications to determine eligibility and continued eligibility in the NEXUS program as described in the *Presentation of Persons (2003) Regulations*. My contact information may also be used by the CBSA to send me notifications related to changes to the NEXUS program.

In addition, I understand that my personal information gathered for the purposes of this application, including my supporting documentation, background information, biometric data, and any other information obtained and collected for the purpose of the operation of the NEXUS program and to conduct applicable checks and verifications to determine my eligibility and continued eligibility in the NEXUS program, may be accessed and used by the CBSA, as well as by other government departments or agencies in Canada (including the Royal Canadian Mounted Police and the Canadian Security Intelligence Service), in accordance with the *Privacy Act*.

In addition to the above-noted use by the CBSA and other Canadian government departments and agencies, I also understand that the CBSA will share its determination of my eligibility to the NEXUS program, based on Canadian criteria, with the United States Department of Homeland Security (DHS). The DHS will, in turn, disclose to the CBSA its determination of my eligibility based on the American criteria.

If you do not consent to the above-noted collection, use and sharing of your personal information, your application cannot be processed and an authorization cannot be granted.

Do you consent to the above-noted collection, use and sharing of your personal information AND do you certify that all the information given on this application, and in support of this application, is provided voluntarily and is true, accurate and complete and that you have read, understood, and agree to abide by all conditions applicable to the program to which you apply and to the use of the associated authorization, including all instructions and notices accompanying this application? ☐ Yes ☐ No

Recommendation: No further recommendations have been made

LIMITING COLLECTION

Risks and Mitigations Strategies

Risk #4: There is a small risk that the CBSA may ask for more personal information than is necessary when a client applies to the NEXUS program.

Mitigation: The following chart describes the data elements that are collected from the NEXUS client's application form and the reason(s) for their collection:

Personal Information Element	Personal Information Sub-Element	Purpose/Necessity of Element
Name	First name/middle name/ last name/nickname/other names	To identify clients
Gender	Male/Female	To identify clients
Date of Birth	Month/Day/Year/ Birth certificate information	To identify clients
Birth certificate number	Birth certificate number and document	To provide proof of citizenship and birth

Place of Birth	City/Province or State/Country	To identify the individual and eligibility in the program
Citizenship Status	Citizenship in Canada or the U.S.; citizenship and/or nationality of third country that has an arrangement with the NEXUS program	To provide proof of identity and citizenship status
Citizenship Document / Naturalization Certificate number and document / Visa/Permit / Permanent resident document	Citizenship Document / Naturalization Certificate number and document / Visa/Permit / Permanent resident document	To provide proof of identity and citizenship status
Passport or Travel document number (and photocopy of document)	Passport number / Travel document number / Photocopy of document	To provide proof of identity, citizenship, and to determine eligibility in the program
Driver's License and number	Driver's License and number	To provide proof of identity and to determine eligibility in the program
Home address / Previous address	Street name/street number/city/ province or state/postal code/country/ telephone number/business phone number/e-mail address/ From date/To date	To contact clients and to assist in performing checks in determining eligibility in the program
Work History	Employer name/street address/ city/province or state/postal code/country/phone number/ type of occupation/ From Date / To Date	To assist in performing checks in determining eligibility in the program
Iris scan / Photograph	Iris scan / Photograph	To identify clients upon entry into Canada as being a trusted member of the program
Credit card information	Credit card information	To collect payment for inclusion in the program
Signature	Signature	Collected along with the credit card info for payment purposes; to record certification that application info provided is true and accurate
Criminal checks/history	Criminal history information	To determine eligibility in the program
Immigration checks/history	Immigration history information	To determine eligibility in the program
Trilateral Trusted Traveller Arrangement – confirmation that an applicant is a member of their own trusted traveller program (done thru GOES by U.S. CBP)	Yes/No	To determine eligibility
Trilateral Trusted Traveller Arrangement – Visa number / photocopy of visa	Visa number / photocopy of visa / electronic travel authority	To provide proof of identity and citizenship and to determine eligibility in the program

Recommendation: No further recommendations have been made

LIMITING USE, DISCLOSURE AND RETENTION**Risks and Mitigations Strategies**

Risk #5: Personal information could inadvertently be used for purposes other than those for which consent was given by the individual to whom it pertains. The program collects personal information for use in determining the application, including risk assessment and admissibility, and in maintaining the membership over its term, including enforcement and program integrity activities. There is a minimal risk that the personal information could be used by accident for another purpose.

Mitigation: CBSA adheres to strict controls over how personal information can be used after it is collected. CBSA will ensure that any use of the information beyond the uses for which it was collected, for example, for law-enforcement or national defence purposes, are in accordance with the appropriate legislation (e.g. section 107 of the *Customs Act*). At this time, the CBSA does not disclose any NEXUS membership information to third party providers and no changes to this policy are anticipated in the future.

The paper-based NEXUS application form also specifically notes that personal information may be shared with other government departments in accordance with the *Privacy Act* (Schedule C). The electronic version on GOES was also updated on October 18, 2016, to reflect this wording.

Recommendation: No further recommendations have been made

Risk #6: Customs information might be misused for a purpose other than that for which it was collected. However, the risk of this occurring has been assessed as minimal. Therefore, there is minor concern that customs information that is disclosed under the provisions of section 107 of the *Customs Act* for a particular purpose may be used by the recipient for other, unauthorized purposes.

Mitigation: Use of information has tight controls. Only the absolute minimum required amount of customs information (for which requestor can demonstrate need) is collected. The information will only be provided for the purposes for which the legal entitlement exists. CBSA personnel are informed of their responsibility to protect personal information. All personnel who collect or handle personal information are screened to the appropriate level.

Recommendation: No further recommendations have been made

Risk #7: Personal information might be improperly disclosed to a third party. Therefore, there is a minor risk that personal information regarding program members might be disclosed to a party who is not authorised to use the information, and who might use it for purposes for which consent has not been obtained is considered minimal.

Mitigation: Processes are in place to ensure that personal information is not inadvertently released to third parties who are not authorized to use the information. Information security measures are in place in accordance with Treasury Board policy, to protect information storage systems from unauthorized access. NEXUS program personnel understand their responsibility to ensure that information is not

shared with unauthorised third parties. The MOU with CBP regarding information sharing sets out limits how CBP may use the information share with it by CBP and who may use the information (Schedule A).

Recommendation: No further recommendations have been made

ACCURACY

Risks and Mitigations Strategies

Risk #8: Personal information collected about an individual might not be accurate. There is a minimal risk that this could occur; nevertheless, as this information could potentially impact an individual's access to services or admissibility to Canada, it is important that there be a process for individuals to obtain and review the personal information collected about them.

Mitigation: NEXUS is subject to ATIP inquiries from individuals who wish to obtain access to their personal information in order to make corrections. Members can also contact the program directly, through the EC and CPC offices to update their personal information and make any corrections. There are processes in place for officers in the field to request corrections to data if an error is detected that cannot be easily resolved. An automated log is also in place to track all changes to personal data in case of an accidental or erroneous change. Should there be a dispute about information collected concerning a member, for example an enforcement record that is impacting their membership to the program, the member may appeal to the Recourse Directorate for adjudication of their claim. Clients are informed of their right to access their information via the privacy statement on the paper and on-line versions of the NEXUS application.

Recommendation: No further recommendations have been made

Risk #9: Kiosk Replacement Project

Information Technology Risk

The NEXUS kiosks had been in operation since 2003 and were at the end of their life cycle that could have resulted in critical equipment failure and could have jeopardized the delivery of the NEXUS program.

Mitigation

The CBSA has replaced the previous trusted traveller kiosks with new modular, scalable, interoperable kiosks that operate using sound proven technology. The next generation of NEXUS kiosks are more secure from tampering or manipulation and more accurate when identifying members because the NEXUS membership card is used with iris biometrics to determine the identity of the traveller and to authenticate that they are a NEXUS member in good standing. Therefore, the risk of non-NEXUS members using the kiosk for entry would be virtually eliminated.

A Threat and Risk Assessment and Statement of Sensitivity for NEXUS Airport Kiosk Passage was performed in 2007 (Schedule RR) but not for the replacement kiosks as far as the Trusted Traveller

Programs unit is aware. Nevertheless, as noted above, the upgrades to the kiosks virtually eliminates the risk of a non-NEXUS member using the kiosk for entry.

Recommendation: No further recommendations have been made

Risk #10: False Matches

Information Technology Risk

There was a remote risk that when an individual presented him/herself at a NEXUS kiosk, the system would falsely match the iris presented with the iris record on file of a different member.

Mitigation

A false match occurred when the old system used to support the NEXUS program matched the iris presented at the kiosk with the file of a different member than the one who presented the iris. This occurred with members wearing designer contact lenses or simply because two members have similar irises on file.

Although incidents of false matches are extremely rare, now that the previous NEXUS kiosks have been replaced and a one-to-one match approach has been instituted, these situations are statistically non-existent. A one-to-one search utilizes a trigger, such as the presentation of a membership card, which then initiates the process so that the system knows that it must compare the iris captured against the iris on file of that specific member thus reducing the potential for any false matches.

Recommendation: No further recommendations have been made

SAFEGUARDS

Risks and Mitigations Strategies

Risk #11: Personal information in transit might be intercepted by unauthorised parties. Therefore, program activities require that information be transmitted using information technology system safeguards to eliminate the interception of NEXUS membership information by an unauthorised party and used for an unauthorised purpose.

Mitigation: The CBSA has developed a disclosure policy and guidelines to cover the use and safeguarding of membership information to eliminate the interception of NEXUS membership information by an unauthorised party and used for an unauthorised purpose. CBSA information technology systems are maintained to a high standard with security a foremost priority. Security measures and protocols are in place to protect the confidentiality of electronic communications. These are subject to on-going review to ensure they continue to properly protect data. Program personnel understand their responsibility to use only secure Information Technology systems to store and transmit personal information in accordance with Treasury Board policy. Communications with CBP are made using encrypted transmissions over a dedicated, secure data link. The information-sharing agreement with CBP set out how information may be transmitted. They also maintain high standards of information

technology and communications security and use only secured systems to handle personal information with other U.S. government agencies.

It should be noted that an IT Security Consultation Report was prepared in 2015 that indicated that IPIL Highway Application was a high risk (Schedule T). It notes that one of the risk factors was the lack of failover capacity which has now been mitigated by the Data Centre Recovery Project. It also notes that the security risks of ICS are directly inherited in the security posture of IPIL Highway and will factor in when IPIL Highway will be re-assessed.

Recommendation: No further recommendations have been made

Risk #12: Traveller Declaration Cards

Privacy Risk

The online Traveller Declaration Card (TDC) requires members' names, credit card numbers and other personal information. There is an outside risk that the TDCs could inadvertently be lost or temporarily misplaced during transportation from the collection boxes to the CPC for storage or follow up administrative purposes.

Mitigation: When a NEXUS member completes and drops off their TDC in the collection box, steps are taken against documents being improperly handled from their removal from the collection boxes to their mailing to the CPC for storage and follow up administrative purposes.

Storage and access to the TDC's require tight controls. CBSA personnel who handle the TDC's are informed of their responsibility to keep them safeguarded and are screened to the appropriate level. The standard operating procedures for handling TDCs include the following with regard to mailing Protected B documents:

- TDCs should be placed in two sealed envelopes for forwarding to the respective CPC located in Niagara Falls, ON, Montreal, QC, or Surrey, B.C.
- The name of the port should also be identified on the inside envelope for statistical purposes.
- The use of two gum-sealed envelopes for internal mailing should be followed as per security policy for Protected B information.
- A security marking should appear on the inner envelope only, while the address should appear on both envelopes.
- The inner envelope should also be marked: "To be opened by addressee only".

If officers who handle the TDC's have any questions regarding the handling and transporting of TDC's, they may address them to the CBSA's Help Desk at AIS.HelpDesk@cbsa-asfc.gc.ca.

Recommendation: No further recommendations have been made

Risk #13: No Threat and Risk Assessment has been completed for the RFID Processor which will allow the CBSA to read RFID-enabled documents including NEXUS cards. A TRA verifying the risks associated with reading RFID-enabled documents has not yet been completed.

Mitigation: To address this, the CBSA is in the process of completing a TRA. The completion date is not yet known, however, the process has been started. Should recommendations come out of the TRA, they will be addressed at that time.

Risk #14: The installation of the RFID readers, including the construction of the required infrastructure, has begun. Given the lack of a TRA supporting the usage of RFID technology, the risk to personal information has not yet been assessed.

Mitigation: To address this, the CBSA is in the process of completing a TRA. The completion date is not yet known, however, the process has been started. Should recommendations come out of the TRA, they will be addressed at that time.

Risk #15: No TRA has been completed for the NEXUS program verifying the risks associated with NEXUS.

Mitigation: NEXUS is a voluntary program designed to expedite passage for low-risk travellers. To address the lack of a TRA, the CBSA is in the process of completing a TRA. The completion date is not yet known, however, the process has been started. Should recommendations come out of the TRA, they will be addressed at that time.

OPENNESS

Risks and Mitigations Strategies

Risk #16: Individuals might not use the NEXUS program if they do not have confidence that their personal information will be safeguarded. This risk is considered low. There is a minimal risk that NEXUS could be perceived negatively if potential applicants are not satisfied with the measures taken to protect their information. The CBSA will ensure that this concern is addressed to the greatest extent possible.

Mitigation: Individuals must understand where and how their information is collected and stored, as well as what measures are being taken to secure their information. The CBSA has endeavoured to address this concern by ensuring that the Canadian and U.S. Privacy Statements are included on both the paper and the on-line NEXUS application form. The privacy statements clearly explain how the information will be shared with other government agencies in Canada and the U.S. Pursuant to these measures, the risk of negative perceptions about proper safeguards for personal information is minimal. In addition, the CBSA has embedded a direct link to the Canadian and U.S. Privacy Statements on the homepage for NEXUS at www.nexus.gc.ca.

Recommendation: No further recommendations have been made

Risk #17: There is a risk that the Privacy Notice Statement and the Consent Statement provided to applicants are not as clear and thorough as they should be.

Mitigation: The text has been amended in accordance with the CBSA's October 2012 letter to the OPC which recommended that "CBSA update their privacy notice to provide more information to applicants on the specific Canadian government organizations to which personal information may be disclosed and

the purposes for disclosure." The CBSA has revised the NEXUS application form to include the specific Canadian government organizations to which personal information may be disclosed and the purposes for disclosure. The Statement now reads as follows:

Canada's Privacy Statement

The information you provide in your application, including supporting documentation and biometric data, is collected by the Canada Border Services Agency (CBSA) and is protected pursuant to both the *Customs Act* and the *Privacy Act*. In accordance with Canadian laws and regulations, this information will be shared with other government departments or agencies in Canada and the United States of America for the purpose of the operation of the NEXUS program and to conduct applicable checks and verifications to determine your eligibility and continued eligibility in the NEXUS program. If the required information is not provided, your application may not be processed and the authorization may not be granted.

Individuals to whom the information relates have rights of access to, correction of and protection of, their personal information under the *Privacy Act*. The information collected is described in Personal Information Bank # CBSA PPU 031. Instructions for obtaining information are provided in Info Source, which is available at public libraries, government public reading rooms and on the Internet at: <http://infosource.gc.ca>

Consent Statement

I understand that any information gathered for the purposes of this application, including any supporting documentation, background information, biometric data and information obtained from the relevant files of law enforcement agencies, including intelligence gathered for law enforcement purposes, will be used for the purpose of the operation of the NEXUS program and to conduct applicable checks and verifications to determine eligibility and continued eligibility in the NEXUS program as described in the *Presentation of Persons (2003) Regulations*. My contact information may also be used by the CBSA to send me notifications related to changes to the NEXUS program.

In addition, I understand that my personal information gathered for the purposes of this application, including my supporting documentation, background information, biometric data, and any other information obtained and collected for the purpose of the operation of the NEXUS program and to conduct applicable checks and verifications to determine my eligibility and continued eligibility in the NEXUS program, may be accessed and used by the CBSA, as well as by other government departments or agencies in Canada (including the Royal Canadian Mounted Police and the Canadian Security Intelligence Service), in accordance with the *Privacy Act*.

In addition to the above-noted use by the CBSA and other Canadian government departments and agencies, I also understand that the CBSA will share its determination of my eligibility to the NEXUS program, based on Canadian criteria, with the United States Department of

Homeland Security (DHS). The DHS will, in turn, disclose to the CBSA its determination of my eligibility based on the American criteria.

If you do not consent to the above-noted collection, use and sharing of your personal information, your application cannot be processed and an authorization cannot be granted.

Do you consent to the above-noted collection, use and sharing of your personal information AND do you certify that all the information given on this application, and in support of this application, is provided voluntarily and is true, accurate and complete, and that you have read, understood, and agree to abide by all conditions applicable to the program to which you apply and to the use of the associated authorization, including all instructions and notices accompanying this application? ☐ Yes ☐ No

Recommendation: No further recommendations have been made

Risk #18: There is a risk that the NEXUS Personal Information Bank (PIB) is not as clear and thorough as it should be.

Mitigation: The text has been amended in accordance with the CBSA's October 2012 letter to the OPC which stated that it would "...amend its Personal Information Bank to better reflect the information sharing activities". The draft revised PIB is included in Section 1 of this PIA.

Recommendation: No further recommendations have been made

INDIVIDUAL ACCESS

Risks and Mitigations Strategies

Risk #19: Individuals may not be properly informed of their right to access information collected by the NEXUS program, or may be aware of their right but not be properly informed of the process. This risk is considered low because the Canadian Privacy Statement embedded in both the paper and the on-line versions of the NEXUS application inform prospective members that:

- The information they provide on the form, including supporting documentation and biometric data is collected by the CBSA and is protected pursuant to both the *Customs Act* and the *Privacy Act*;
- The information will be shared with other government departments or agencies in Canada and the United States of America for the purpose of the operation of the NEXUS program and to conduct applicable checks and verifications to determine their eligibility and continued eligibility in the program;
- The information collected is described in PIB #CBSA PPU 031;
- Instructions for obtaining information are provided in Info Source, which is available at public libraries, government public reading rooms and on the Internet at <http://infosource.gc.ca>.

There is no published national procedure requiring the program's employees to inform clients of their right to access information. The NEXUS program's SOPs do not mention Privacy considerations.

Mitigation: A direct link to the Privacy Statements can now be found on the homepage for NEXUS (www.nexus.gc.ca) on the CBSA external website in order to improve access to this information.

In addition, a revised PIB is included in Section 1 of this PIA.

Recommendation: No further recommendations have been made

Risk #20: Individuals will not have access to their personal information if that information is required. This risk is considered low. Individuals have the right to access their personal information upon request. There is a remote possibility that personal information collected by CBSA may not be available upon request due to some type of systems failure.

Mitigation: Audit trails are built into all information technology systems, including log systems in the passage facilitation technology, and logs of all activities which affect the personal information saved to an individual's record. All systems are backed up and personal information retained in accordance with CBSA policies.

Clients may also access and correct their personal information by attending in person at an EC or electronically through GOES.

Recommendation: No further recommendations have been made

CHALLENGING COMPLIANCE

Risks and Mitigations Strategies

Risk #21: There is an outside risk that an individual might challenge the CBSA to demonstrate how it complies with its responsibilities under Privacy legislation. It is possible that an individual may submit a claim that the CBSA has not taken sufficient measures to satisfy their privacy obligations. The Agency would develop communications material to explain how it adheres to the legislation and regulations (e.g. subsections 107 (4) (5) (6) (8) and (9) of the *Customs Act*). The CBSA's Policy on the Disclosure of Personal Information has been made available to the general public as evidence to attest to the fact that appropriate privacy protection processes are being fully implemented (see Schedule K).

Mitigation: Any related challenges will be processed by the ATIP Division, who is responsible for ensuring that the public understand how the Agency complies with the provisions of the *Access to Information Act*, the *Privacy Act*, and fulfills its responsibilities under the *Customs Act*.

Recommendation: No further recommendations have been made

Summary of Identified Risks (example):

1 - Accountability	1	2-3 Activity Partners	
2 - Identifying Purposes	2	2-1 Type of Program or Activity; 5-9.4 Use of Personal Information.	
3 - Consent	3	5-5.2 and 5-5.3 Indirect Collection with Consent	
4 - Limiting Collection	4	2-2 Type of Personal Information and Context; 3 Analysis of Personal Information Analysis; 5-3.6 Authority for Collection of Social Insurance Number	
5 - Limiting Use, Disclosure and Retention	5	2-3 Activity Partners	
	6	2-3 Activity Partners	
	7	6 - Summary of Analysis and Recommendations	
6 - Accuracy	8	6 - Summary of Analysis and Recommendations	
	9	6 - Summary of Analysis and Recommendations	
	10	6 - Summary of Analysis and Recommendations	
7 - Safeguards	11	2-7 Personal Information Transmission	
	12	5-12 and 5-13	
		14 Safeguards - Administrative, Physical and Technical	
	13	6 - Summary of Analysis and Recommendations	
	14	6 - Summary of Analysis and Recommendations	
	15	6 - Summary of Analysis and Recommendations	
8 - Openness	16	6 - Summary of Analysis and Recommendations	
	17	6 - Summary of Analysis and Recommendations	
	18	6 - Summary of Analysis and Recommendations	
9 - Individual Access	19	6 - Summary of Analysis and Recommendations	
	20	6 - Summary of Analysis and Recommendations	
10 - Challenging Compliance	21	6 - Summary of Analysis and Recommendations	

SECTION 7 - SUPPLEMENTARY DOCUMENTS LIST

List all supplementary documents that support the conclusions of this CBSA PIA. For each document, cite the specific sections of the documents (subject, chapter, page, paragraph, etc.) that correspond with the CBSA PIA and link them to the PIA sections.

Document	Document Reference	PIA Reference
MOU for the Disclosure of Information for the purposes of the Joint Alternative Presentation and Inspection Programs between CBSA and CBP	Parts D & E	Introduction Part 2 10.1.4 Section 6, Risk #7 Annexes D & H
NEXUS Personal Information Bank	All sections	Introduction Section 6, Risks #2, 15 & 16
NEXUS Application Form	Sections A, B, C, F & G	Introduction #2 & Part 1 s.4 - Notice s.5, 5.3 s.6, Risk #'s 2, 5, 13 & 14
Privacy Statement	All sections	s.4 – Explanation of the Process & Notice s.5, 5.1 Risk #'s 8, 13, 14 & 16 Annex H, #1
Traveller Declaration Card	Sections A, B, C, E & F	s.4 – Credit card info & Notice Risk #12 Annex F
Admissibility Complaint Policy of the CBSA People Processing Manual	First section	Nil
NEXUS Privacy & Consent Portions of the Application Form	All sections	Introduction, Part 4 s.2, Part E
Policy on the Disclosure of Customs Information	Pages 7 & 12	s.5, Parts 9.4 & 11.1
Trusted Traveller Programs Cancellation/Rejection Letters	All sections	Part 4, CBSA Revocation of NEXUS Privileges Flowchart
Policy on the Retention of Payment Card Information	Section 2	s.4 – Credit card info & part 7.3
Policy on the Disclosure of Personal Information	Pages 5, 7 & 21	s.6 – Risk #18
GEC-GES Interface Specifications	Page 8	Nil
Print Screens Global Enrolment NEXUS On-line Application Form	All sections	Nil
Data Matching – On-Line NEXUS Application	Sections 1, 3 & 4	Definitions s.2 – 6.3.3

		s.5 – 8.1.2 & 8.1.4
Interconnection Security Understanding	Sections 1 & 2	Nil
Business Use Cases	Sections 1 & 2	Introduction, #4
TRA and SoS for Global Enrolment Component	Sections 7 - 14	s.5 - 12.1 & 13.1
Integrated Customs System – Use Case	Sections 1, 3 & 4	Executive Summary s.1 s.4, #1 s.6, Risk #2
NEXUS IT Security Consultation Report	Nil	s.6, Risk #11
GEC Restructuring	Nil	Nil
TRA and SoS for Trusted Traveller Programs	Pages 4, 5, 6	s.5, 12.1 & 13.1
TRA and SoS for Passage – NEXUS Air Pilot Project	Pages 3 – 7	s. 5, 12.1 & 13.1
NEXUS Highway Technology Design Document	Pages 3, 4, 5, 24, 25 & 26	Nil
NEXUS Air Pilot Project Charter	Page 4	Nil
NEXUS Marine Project Charter	Page 4	Nil
TRA and SoS for NEXUS Highway	Pages 3 – 6, 27	s.5, 12.1 & 13.1
TRA and SoS for NEXUS Highway Passage (2003)	Pages 3 – 7, 26	s.5, 12.1 & 13.1
SLA Between ISTB and Programs Branch for NEXUS Highway	Pages 1 & 8	Nil
TRA and SoS for NEXUS Highway Passage (2005)	Pages 4 – 7, 12	s.5, 12.1 & 13.1
NEXUS Highway Application SoS	Sections 2 & 3	s.5, 12.1
NEXUS Highway Passage TRA	Sections 2, 3, 5 & 6	s.5, 12.1 & 13.1
Peace Bridge NEXUS eGate SOPs	Pages 1 - 2	Introduction, #3
Peace Bridge NEXUS eGate Mock-up Drawing	Full diagram	Introduction, #3
eGate Network Diagram	Full diagram	Nil
NEXUS eGate Business Requirements for Proof of Concept	Sections 1 – 4, 12	Introduction, #3
E-Gate Interim Report	Sections 1, 3, 4 & 6	Nil
Policy on the Overt Use of Audio-Video Monitoring and Recording Technology	Pages 3 – 7, 11, 13, 14	Introduction, #3 s.1 s.2, 6.3.2 s.5, 16.4
NEXUS eGate Process Flow	Pages 1 – 2	Introduction, #3
MoU Between the CBSA, U.S. CBP and Mexico's INM	Pages 2 – 3	Introduction, #2 s.2, Part C
Operational Program Plan	Sections 2, 3, 5, 6, 11, 12, Annex 1	Introduction, #2 Annexes D, E, F, G & H

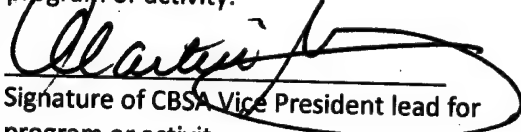
NEXUS Program

PIA

Business Use Case – TTP – Entry Into Canada – Kiosk	Sections 1 & 2	Nil
TTP Kiosk – Technology Architecture Design	Sections 2, 6 & 7	Introduction, #4
TRA and SoS for NEXUS Airport Kiosk – Passage	Pages 4, 8, 13, 34 & 35	s.5, 12.1 & 13.1
Service Level Objective (SLO) for the TTP Kiosk	Page 4	Nil
MoU Between the CBSA and CATSA	Sections 1, 3, 4, 5 & 6	Introduction, #1 s.4, #6
Trusted Traveller CATSA Line Automated Gate Solution	Full diagram	Introduction, #1 & Parts 1, 2&3 s.2, 6.3.1 s.4, #6
CATSA Statement of Sensitivity	Sections 2, 3, 4 & 8	s.5, 12.1
CATSA Service Level Agreement	Sections 2 & 4	Introduction, #1 s.4, #6

SECTION 8 - FORMAL APPROVAL

The following signature represents a commitment to comply with sections 4 to 8 of the *Privacy Act* and the related privacy policy requirements outlined in the CBSA PIA as they relate to the administration of the identified program or activity.


Signature of CBSA Vice President lead for program or activity

2017-01-04
Date

Note: Responsibility for sections 4 to 8 of the *Privacy Act* rests with all employees of government institutions that handle personal information. Officials who manage such programs and activities are responsible for ensuring that such requirements are implemented as part of the administration of the program or activity.

The following signature represents a commitment by the Head of the institution or his/her delegate(s) who is responsible for establishing personal information banks in accordance with section 10 of the *Privacy Act*.


Signature of CBSA ATI and Privacy Director

2016-12-19
Date

Note: Under the *Privacy Act*, the Head or his/her delegate(s) is responsible for complying with legal and relevant privacy policy requirements related to the approval and registration of personal information banks

Note: The table below must be used to keep an account of actions completed and to track outstanding actions required to achieve privacy compliance:

Canada Border Services Agency

Privacy Compliance Analysis question #	Action required to support legal and policy compliance (cross reference to relevant question of Section 5 – Privacy Compliance Analysis)	Done	To be done
	retention period established by the Privacy Regulations. c) Reference to the RDA, the retention period and the disposition standards for the program have been cited in the relevant PIB.		
8	Controls and procedures are in the process of being implemented to ensure that the personal information associated with the program is as accurate, complete and up-to-date as necessary.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Other Privacy Considerations related to specific principles that are not explored in the previous 17 sections (these considerations should be explored in the Executive Summary)			
Openness	Describe how the results of any privacy impact assessment or audit will be made available to the public. The Executive Summary will be published on the external CBSA ATI and Privacy Division website at http://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/pia-efvp/atip-aiprp/pias-sefp-eng.html	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Are policies and practices relating to the proposal's management and handling of personal information available to the public?	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Is there a communications plan to explain to the public how personal information will be managed and protected?	<input type="checkbox"/>	<input checked="" type="checkbox"/>
	Is there a clearly defined and easy process for individuals to access such information and/or communicate with appropriate individuals with respect to policies and practices relating to management and protection of personal information?	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Where appropriate, will public consultation take place on the privacy implications of the proposal?	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Individual's Access to Personal Information	Is the system designed to ensure that an individual can have access to his/her personal information, including all other programs or applications that have received copies of the information? s. 12(1)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Are there documented procedures developed or planned on how to make privacy requests or requests for the correction of personal information? s. 12 (2)	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Privacy Compliance Analysis question #	Action required to support legal and policy compliance (cross reference to relevant question of Section 5 – Privacy Compliance Analysis)	Done	To be done
	Are individuals provided with access to their personal information in the official language of their choice? s. 17(2)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	If appropriate, are individuals provided with access to their personal information in an alternative format? s. 17(3)	<input type="checkbox"/>	<input checked="" type="checkbox"/>
Challenging Compliance	Are the complaint procedures for the proposed program or service consistent with legislated requirements? s. 29-35	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	To improve information management practices and standards, has a procedure been established to log and periodically review the nature, frequency and resolution of complaints?	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Are there oversight and review mechanisms implemented or available to ensure accountability?	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Have oversight agencies, including the Office of the Privacy Commissioner, issued reports or opinions on issues that would be relevant to the proposal?	<input type="checkbox"/>	<input type="checkbox"/>

Annex B: Office of the Privacy Commissioner Expectations

In their March 2011 document, *Expectations: A Guide for Submitting Privacy Impact Assessments to the Office of the Privacy Commissioner of Canada*, the OPC has expressed the importance of analysing the risks of the project, program or initiative against the ten universal privacy and fair information practice principles of the Canadian Standards Association Model Code for the Protection of Personal Information.

The most relevant demonstration of the privacy risk and compliance analysis is the action plan. The OPC has said the following in their **Expectations** guide with respect to the action plan:

Once privacy risks and their proposed mitigating measures have been identified, we expect to see an Action Plan drawn up by the institution, indicating a specific time frame for remedying or mitigating the risks that have been identified, and if possible, naming a specific person or staff position accountable for taking action.

The action plan must list all privacy risks and compliance issues identified in the PIA and supplementary documentation. All risks and issues must be organized by the 10 universal privacy principles.

All recommendations and proposed mitigation strategies must also be described in the action plan. Identify the responsible program area and the timeline for completion or implementation of the strategy. The ATI and Privacy Division will provide programs with an action plan template to be addressed near the end of the PIA process.

The expectations of the OPC for each privacy principles are included below for your reference.

Accountability

Under this principle the OPC would expect to see documentation of an administrative structure for privacy, including input from legal services, access to information and privacy and information technology branches within an institution, with defined processes for determining when new projects require PIAs, for carrying them out, implementing mitigating measures and auditing for assurance of compliance. We expect PIA reports to be signed off at the appropriate level, and that training in privacy issues and procedures has been documented and is refreshed with employees regularly; and that privacy protective language is included in all contracts with third parties handling personal information in accordance with TBS guidance documents and internationally accepted best practices; and that regularly scheduled privacy compliance audits will be undertaken and the findings acted upon.

Identifying Purposes

The *Privacy Act* restricts federal government institutions to the collection of personal information that relates directly to an operating program or activity of the institution, so we would expect to see a clear description of the program and why each piece of information is needed; a description of the legislative authority for the collection; a clear listing of all the data elements collected; copies of any relevant documents such as application forms identifying the purpose for the collection or on-line notices of use; a copy of an up to date PIB description; a statement of any proposed new consistent use of information previously collected and a clear rationale as to how the use is reasonable and directly connected to the

original collection -- this may include an analysis of how an individual to whom it relates would reasonably expect it to be used for that purpose; a statement outlining any intended secondary uses of the information; whether the information is collected directly from the individual and if not, why; and a description of how personal information used for planning, forecasting or statistical purposes would be anonymized or de-linked from individual identifying information.

Consent

This is closely tied to the Identifying Purpose principle. Under this principle, OPC would expect to see a copy of notification language on forms or websites; a clear description of the purpose for collection; a rationale for not seeking consent, as is provided for in the *Privacy Act*; for web sites, a copy of the Privacy Notice Statement under which personal information is submitted to the institution.

Limiting Collection

Under this principle, OPC would expect to see a clear justification of the need for each data element collected, in keeping with the requirement of the *Privacy Act* that no personal information is to be collected by a government institution unless it relates directly to an operating program or activity of the institution; an indication that a data minimization exercise has been undertaken to ensure that each data element is necessary and that this exercise will be refreshed regularly; and that information collected from another department for a secondary use will be purged of all but the essential data elements before use.

Limiting Use, Disclosure and Retention

Under this principle, OPC would expect to see a description of the specific uses and proposed disclosures of the information; a clear statement limiting the use of the information to the purposes identified; a clear retention policy and disposition schedule that is also noted in the PIB; a process for destruction of the information that is in keeping with the *Privacy Act* and Regulations; copies of MOUs or agreements with third parties to whom information is disclosed governing its use, retention and disclosure, and clauses with contractors or sub-processors of information indicating the originating institution has the right to audit for compliance with privacy provisions.

Accuracy

Under this principle, OPC would expect to see a description of the process used by entities to ensure accuracy, particularly when administrative decisions are made; a description of how changes to records are logged and monitored; a statement of whether automated decision-making based on risk profiles is being undertaken and how automated decisions are vetted for accuracy; an explanation of the processes open to individuals seeking to correct information; a description of the process by which second or third parties to whom information has been disclosed will be notified of changes and corrections to the record; and a description of how audit trails of records transactions are monitored and evaluated.

Safeguards

OPC would expect to see under this principle a description of the physical and electronic safeguards that are in place to protect information; a Threat & Risk Assessment (TRA) with emphasis on privacy risks and concerns and a discussion of how these concerns have been remedied or addressed; a notation that encryption is used for personal information both in transit and at rest; a description of how system logs of information transactions are monitored for inappropriate use, including viewing of the information;

strong electronic access control, including controls on remote access, and the use of mobile devices; policies for the use of portable storage devices such as flash drives; a description of role-based access controls; and a description of the steps taken to ensure complete destruction of the information at the end of its life cycle.

Openness

Under this principle, OPC would expect to see a summary of the PIA written in plain, understandable language, posted on the institutional website in a manner accessible to the general public and containing a link to the relevant PIB description in CBSA Info Source; for particularly sensitive or privacy invasive programs we would expect to see the public communications plan described in the PIA, including a variety of methods such as posters, brochures and media announcements as well as detailed discussion of the PIA in the institution's Annual Report under the *Privacy Act*; a description of consultations with key stakeholders and the privacy risks or concerns raised should be readily available on the website; the name and contact information of an individual accountable for the handling of personal information should be easily obtained through the website or by calling the institution's main public number.

Individual Access

Under this principle, OPC would expect the PIA to include a description of any informal process the CBSA may have in place for access to and correction of personal information; an up to date and comprehensive description of information contained in the PIB corresponding to the initiative; a description of the process by which information in the hands of third parties is corrected following requests; a description of how the general public is made aware of these processes, for example, by a link and/or a toll-free number shown on the home page of the institutional website.

Challenging Compliance

OPC would expect to see the PIA address this principle by indicating clearly who is responsible for receiving and resolving privacy complaints; describing complaints that may have been received in any similar activity or pilot project and how they were handled; including privacy issues in project evaluations or feasibility reports; describing how and when compliance audits for privacy will be undertaken; including information on how to file a complaint with OPC under the *Privacy Act*; and reporting in some detail on specific and/or systemic privacy issues in its Annual Reports.

Annex C: Categories of Personal Information

The **Description** section in a PIB describes the personal information in the records to which the bank relates. TBS has established the following categories of personal information, which give examples of specific elements of personal information that fall under each category. The purpose of the categories is to reduce the number of personal information elements that need to be listed in the Description section. These categories are representative of the personal information collected by most institutions, and they now appear in many of the CBSA registered PIBs. The ATI and Privacy Division modified the original list to reflect CBSA business lines.

Biographical information (e.g. work history, curriculum vitae, family information, Passenger Information, etc.)

Biometric information (e.g. blood type, eye or facial scan, DNA, finger / hand prints, etc.)

Contact information (e.g. work and / or home information, including postal and e-mail addresses, telephone, fax, cell phone numbers, etc.)

Citizenship status or Nationality (e.g. citizen, landed immigrant, etc.)

Crew detailed information

Criminal checks / history (e.g. information related to criminal record checks, investigations, charges, conviction dates and locations, pardons, etc.)

Date of birth

Date of death

Destination City

Employee identification number (e.g. Personal Record Identifier)

Employee personnel information (e.g. records of attendance and leave, notices of disciplinary action, alternative work arrangements, decisions concerning compensation and fitness for work, official languages qualifications, salary, deductions, level of security clearance, performance reviews and appraisals, rating board assessments, including evaluation notes from staffing boards, training and development course applications and evaluations, etc.)

E-Ticket Information

Financial information (e.g. income, investments, mortgages, loans, orders of garnishment, financial institution information for direct deposit and other banking purposes, including name and branch number of institution, account number(s) and name(s) on accounts, etc.)

IBAS Case Number

Gender

Itinerary Cities

Language (e.g. mother tongue, official and other languages, etc.)

Medical information (e.g. psychological assessments, blood type, etc.)

Name (e.g. last name (surname/family name), given names (first, second or more), maiden name, nicknames, aliases, etc.)

Opinion or views of, or about, individuals

Passenger Name

Passport Number or Travel Document Number

Place of ticket purchase

Photos

NEXUS Program

PIA

Physical attributes (e.g. height, weight, color of hair and eyes, physical markings (scars, tattoos, body piercing), etc.)

Place of birth

Place of death

Port of Embarkation and Port of Debarkation

Signature

Social Insurance Number

Special Travelling Considerations such as Employee Pass, Buddy Pass and Parental Passes

Visa Number

Annex D: Controls and Procedures Implemented to Limit Personal Information Collection

Section 5, Question 2.2 requires CBSA to implement controls and procedures to ensure the CBSA does not collect more personal information than is necessary for the identified program/activity and that a continuing need exists for that information to be collected.

This section provides a brief description of the controls and procedures that have been implemented. At a minimum, this section will address the following:

1. Procedures that clearly identify the need to collect, use, and disclose only the information necessary to perform a particular task;
2. Procedures that identify and limit secondary uses of the personal information;
3. Training to staff on those procedures;
4. Regular (at least yearly) audits to ensure staff are abiding by those procedures; and
5. Regular (at least yearly) audits of other institutions' uses and safeguards of personal information shared with them as part of the processes identified in Section 4. Included in these audits is a determination if unauthorized secondary uses or disclosures have been performed by the institution.

The NEXUS program is authorized under subsection 11.1(1) of the *Customs Act* and is also governed by the *Presentation of Persons (2003) Regulations*. The personal information collected will be used solely for the original purpose for which it was obtained which includes making a determination of eligibility into the voluntary NEXUS program or to assess or maintain existing NEXUS membership status. Further, a CBSA-CBP MoU for the Disclosure of Information for the Purposes of the Joint Alternative Presentation and Inspection Programs has been developed that describes the collection, use and disclosure of information for the purposes of the NEXUS program (see Schedule A of Supporting Documentation).

The CBSA cannot collect more personal information than what is asked for in the application form (see Executive Summary for a detailed list of information collected); the information collected assists with the risk assessment and continued risk assessment of the client to ensure they are low risk at time of application and throughout their membership.

All CPC staff are trained on the appropriate procedures for collecting, recording and storing of all personal information for the NEXUS program. Training procedures are retained on the CPC unit's shared-drive for access by new employees and/or workshop training/employee reference and are updated on a regular basis. Audits are conducted regularly to ensure procedures are followed by CPC staff. Formal sampling is conducted bi-annually with results reported to HQ.

Under the Trilateral Trusted Traveller Arrangement, Canada, the U.S. and Mexico are developing controls and procedures with regard to limiting the collection of personal information (an MoU and an Operational Program Plan have been signed). Similar arrangements are being developed with the UK.

Annex E: Controls and Procedures Implemented to Documenting Consent and Withdrawal of Consent

Section 5, Responses 4.3, 4.4, 5.2 and 5.3 require CBSA to implement controls and procedures ensuring the CBSA keeps a record documenting whether or not an individual provided consent when it was sought, including a record documenting any withdrawal of the consent.

This section provides a brief description of the controls and procedures that have been implemented. At a minimum, this section will address the following:

1. The purpose of the consent and the specific personal information involved;
2. When is Consent Required?
3. The sources who will be asked to provide the information, in the case of indirect collections.
4. Purpose of the Consent.
5. Uses and disclosures that are not consistent with the original purpose of the collection and for which consent is being sought.
6. Any consequences that may result from withholding consent.
7. Any alternatives to providing consent.
8. Identify standards and mechanisms that are in place to ensure an individual has the capacity to give consent.
9. If information is being collected from persons authorized to act on behalf of minors, incompetents or individuals who have been deceased for less than 20 years, identify the mechanisms ensuring that such persons are authorized to act on behalf of such individuals who do not have the capacity to provide consent.
10. Procedures for collecting and storing consent (either electronically, paper-based, or both).
11. Procedures for collecting, recording, and storing withdrawal of consent, including notification to the individual of the consequences, if any, of withdrawing consent.
12. Training to staff on those procedures;
13. Regular (at least yearly) audits to ensure staff are abiding by those procedures; and
14. Standards and Mechanisms utilized to validate an individual's legal authority to provide consent for a minor, incompetent person, and deceased person.

To become a member of the voluntary NEXUS program, the applicant must provide consent on the application form (either by signing the paper form in the appropriate space or the filling of a form field for the on-line version). Therefore, the number of applications received would equal the number of consents. Paper-based applications are scanned and an electronic copy of the file is retained at the CPC. The U.S. CBP sends the number of applicants who applied through GOES to the CBSA on a regular basis. To see what personal information is asked on the NEXUS application form, please refer to Schedule C.

Consent is required to ensure that the applicant understands that the information gathered is used for the purpose of the operation of the NEXUS program and to conduct applicable checks and verifications to determine eligibility and continued eligibility in the NEXUS program as described in the *Presentation of Persons (2003) Regulations*.

As noted in the Consent form, if the applicant does not consent to the collection, use and sharing of their personal information, their application cannot be processed and an authorization cannot be granted. When an applicant subsequently advises that they are unwilling to consent to the collection of personal information/data, the applicant is asked to provide a written request, either by e-mail or hard copy through facsimile or post requesting that they are withdrawing their consent. Their correspondence is placed on their file.

Pursuant to sections 7(2) of the *Presentation of Persons (2003) Regulations*, a person may apply for an authorization (NEXUS card) on behalf of a child who is under 18 years of age. Section 7(2.1) deems that "A person may apply for an authorization.....on behalf of a person who is 18 years of age or more who has a mental or physical disability if the person who has the disability consents to the application or, if the person has been declared incompetent, a person who is legally authorized to act on the person's behalf consents to the application."

All CPC staff are trained on the appropriate procedures for collecting, recording and storing of all personal information for the NEXUS program. Training procedures are retained on the CPC unit's shared-drive for access by new employees and/or workshop training/employee reference and are updated on a regular basis. Audits are conducted regularly to ensure procedures are followed by CPC staff. Formal sampling is conducted bi-annually with results reported to HQ.

Under the Trilateral Trusted Traveller Arrangement, Canada, the U.S. and Mexico are developing controls and procedures with regard to documenting consent and withdrawal of consent (the Operational Program Plan is attached at Schedule OO). A similar arrangement is being developed with the UK.

Annex F: Controls and Procedures Implemented for Retention and Disposal of Personal Information

Section 5, Response 7.2 requires CBSA to implement controls and procedures ensuring the CBSA maintains a record of personal information for a minimum of two years following the last administrative action or when the individual has consented to an earlier timeline for disposal.

This section provides a brief description of the controls and procedures that have been implemented. At a minimum, this section will address the following:

1. How the information is collected and maintained – paper and/or electronic storage.
2. Description/Justification of the retention timeframe
3. Description of how the records will be destroyed, including how the CBSA will be capable of determining when the time for disposal has arrived.
4. Description of any information which must be transferred to LAC.
5. Training to staff on those procedures;
6. Regular (at least yearly) audits to ensure staff are abiding by those procedures.

NEXUS Retention Specifications have been developed to ensure that all of the GoC's financial and administrative, legislation and regulatory requirements are complied with (see Schedule J). User activity of GEC and the CPCS within the CBSA can be monitored since the user making the modifications to data and the date and time of the modification are logged. Firewalls are used to protect the integrity of the data storage. Once information is modified by either the CBSA or the U.S. CBP, this information will be updated to other agencies' internal systems.

Further, all CBSA policies relating to data storage, transmission and destruction apply to the personal information collected for NEXUS at enrolment, at the interview stage or at renewal. These policies are set out in the Security Volume of the Comptrollership Manual at http://atlas/cb-dgc/pol/cm-mc/sv-vs/index_eng.asp. A copy of this manual is also available upon request. These policies also relate to the TDC's collected at passage.

Presently, all paper applications and attached documents are scanned into an electronic library with an identification number and client name and may be readily retrieved and/or deleted when the retention period has been reached. Once scanned, the original hard copy of the application/document is shredded. Electronic files are retained for six years. NEXUS memberships are valid for five years – the six year retention timeframe is beneficial to verify data from the previous or initial application when a renewal or re-application is received at the CPC. The virtual filing system has been in operation since April 2012. When the retention period is reached, files may be filtered for destruction by searching the original entry date and/or the "Date Modified" feature.

Audits on storage and maintenance of files are currently conducted on a regular basis to ensure files are scanned, records are complete with all documents and corresponding correspondence in the virtual library and have not yet reached the end of the retention period.

Traveller Declaration Cards are retained in hard copy and archived for seven years, after which time they are destroyed in a secure manner. These practices follow established standards for the handling and destruction of financial documents.

Under the Trilateral Trusted Traveller Arrangement, Canada, the U.S. and Mexico will retain information received for the period stipulated by their respective national laws and applicable national administrative policy. In Canada, pursuant to the *Privacy Regulations*, the retention period is at least two years following the last time the personal information was used for an administrative purpose unless the individual consents to its disposal. At the end of the period for retaining the information, Canada, the U.S. and Mexico will destroy the information. A copy of Mexico's privacy statement for its Viajero Confiable program is included in the Operational Program Plan at Schedule OO. Similar arrangements are being developed with the UK.

CBSA inherited RDA 2000/033 from the CRA and it was within the purview of the CBSA to apply the RDA during the time period ranging from 2003 to March 20, 2015. However, on March 31, 2015, Library and Archives Canada provided the CBSA with its first Disposition Authorization (DA). This institution-specific DA (2015/008) supersedes all authorities used in the past emanating from the CRA or IRCC. Acquiring a new RDA does not nullify the validity of any existing retention and disposition schedules under the previous RDA 2000/033, but they will now be enforced through DA 2015/008. At the end of the retention period, the business owner must complete the "Records Storage or Records Destruction" form and seek approval from the Director of the Office of Primary Interest and the Director of Information Management (IM) for disposition of the records. The IM Director will keep the signed forms for 10 years after the record(s) is/are destroyed as the disposition of information resources of business value must always be documented and approved before action.

Annex G: Controls and Procedures Implemented for Accuracy of Personal Information

Section 5, Response 8.2 requires CBSA to implement controls and procedures when data accuracy measures are adopted with an individual authorized to act on behalf of the individual.

Those controls and procedures must ensure that:

1. the technique(s) and the specific source(s) used to validate or update the personal information are documented;
2. individuals are given the opportunity, whenever possible, to request correction of any inaccurate personal information before the information is used in a decision-making process that affects them;
3. personal information can only be modified or corrected by those within the CBSA who have the authority to do so;
4. when personal information is corrected or annotated, the record of personal information indicates the date of the last correction or annotation and the source of the information used to make the correction or annotation; and
5. when personal information is corrected or annotated, other authorized holders of the information are notified about the correction or annotation and that all copies of the information in the possession of the CBSA are corrected / annotated.

Responsibility for ensuring that the personal information for NEXUS members is accurate, complete and up-to-date rests with the individual member. Program members are informed of their responsibility to update information during the enrolment process. If a member does not update their information, sanctions may be applied as this affects the program's ability to conduct risk assessments to determine on-going eligibility. Information is updated at least every five years when members have the opportunity to renew their membership in the program.

As the responsibility for correcting or updating NEXUS membership in GEC rests with the individual member, the GEC system is not designed to ensure that the individual member is notified of the correction/update. Currently, when a NEXUS member wishes to correct or update their membership information (e.g. change an address or name) they may: request the correction/update electronically via GOES; contact the CPC or EC by facsimile or e-mail to request the correction or update (once received, the updated information is entered into the client profile in GEC and updated documents are scanned and added to the original electronic client file with the original copy being shredded); submit a renewal/re-application that contains corrected/updated information; attend in person at an EC.

Under the Trilateral Trusted Traveller Arrangement, Canada, the U.S. and Mexico have developed controls and procedures with regard to the accuracy of personal information which is included in the Operational Program Plan (Schedule OO). Similar arrangements are being developed with the UK.

Annex H: Controls and Procedures Implemented to Limit Access to Personal Information

Section 5, Response 9.1 requires the CBSA to implement controls and procedures to ensure that access to the personal information is limited to authorized individuals who need to know. These individuals have been identified in Section 4.6 of this PIA.

This section requires a description of the controls and procedures utilized to ensure access is limited and that the employees are aware of and abide by the CBSA's Privacy Code of Ethics.

Personal information can only be disclosed with the express consent of the individual to which that information pertains or pursuant to s. 107 of the *Customs Act*.

1) CBSA:

Access to data records is determined through user profiles. User profiles are used to govern the control and administration of personal and payment information. Only system administrators and authorized CBSA maintenance personnel have access to all data for system maintenance purposes. The number of maintenance users is kept to a minimum. These employees are security screened to the appropriate level and receive security awareness training. Users are limited to accessing only data and services for which they have been authorized. Log records are maintained of all user access and any modifications to an individual's record. These records may be used for audit purposes.

Procedures to identify and respond to security breaches or disclosure of personal information may be found in the CBSA's ATIP procedures. The ATIP unit would also alert the Office of the Privacy Commissioner of any breaches.

All program employees are aware of an individual's right to access their own personal information. Individuals are informed of their rights through the privacy statement on the application form, which explains how the information provided will be used and directs the member to InfoSource.gc.ca for information on how to access their own personal information.

Log records are maintained of all user access and any modifications to an individual's record. These records may be used for audit purposes.

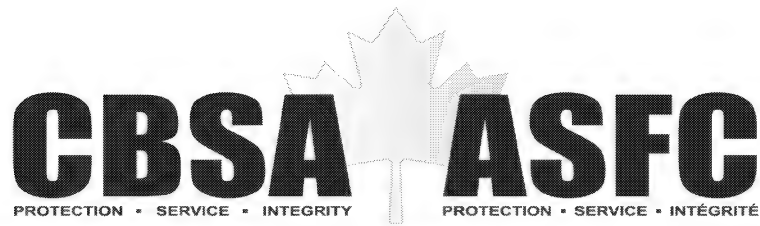
2) U.S. CBP and GPO:

Personal information is shared with the CBP as authorized by the applicant on the application form and is used to determine eligibility and continued eligibility in the NEXUS program. Personal information is also used by the GPO to print and issue the NEXUS card to members. The CBSA and CBP have developed an MoU for the Disclosure of Information for the Purposes of the Joint Alternative Presentation and Inspection Programs that describes the collection, use and disclosure of information (see Schedule A of the Supporting Documentation).

3) Under the Trilateral Trusted Traveller Arrangement, Canada, the U.S. and Mexico have developed controls and procedures with regard to limiting access to personal information.

These are included in the Operational Program Plan at Schedule OO. Similar arrangements are being developed with the UK.

These are included in the Operational Program Plan at Schedule OO. Similar arrangements are being developed with the UK.



Overt Use of Video Monitoring and Recording Technology

Privacy Impact Assessment (PIA)

Border Programs
Programs Branch
November 2013 / Version 14

Change Control Table

Version	Date	Change Made By	Change Requested By	Change
1	Oct. 19/10	Lise Dupuy	Heath Lariviere	Creation of Document First draft
2	Nov. 04 /10	Lise Dupuy	Heath Lariviere and Team	Revisions to content
3	Nov. 16 /10	Lise Dupuy	Heath Lariviere and Rob Gilbert (ATIP)	Revisions to Content /Meeting with Rob
4	Nov. 24/10	Lise Dupuy	Raie Leith	Revision to content (Section 1)
5	Jan. 21/11	Raie Leith	Raie Leith	Complete revision of content, addition of risk mitigation section.
6	Mar. 1, 2011	Raie Leith	Raie Leith	Conversion to new template, content additions.
6.1	Mar. 15, 2011	Raie Leith	Raie Leith	Additions to content.
7	May 5, 2011	Raie Leith	Raie Leith	Conversion to new template, content additions.
8	Aug. 19, 2011	Raie Leith	Raie Leith	Additions to content.
9	July 13, 2012	Darren Okabe	Darren Okabe	Additions to content.
10	July 21, 2012	Lyne Pelletier	Lyne Pelletier	Provide Comments
01	Aug. 01, 2012	Darren Okabe	Lyne Pelletier	Change PIA to video only. Additions to content.
02	Aug. 3, 2012	Darren Okabe	Darren Okabe	Additions to content.
02	Aug. 22, 2012	Lyne Pelletier		Final Review
03	Aug. 27, 2012	Adam Norwick	Dan Proulx	Clarification concerning audio components of video technology
04	Sep. 5, 2012	Darren Okabe	Darren Okabe	Additions to content.
05	Oct. 16, 2012	Maureen Haley	Megan Imrie	Addition to executive summary indicating CBSA will explore audio capture in future

Version	Date	Change Made By	Change Requested By	Change
06	Oct. 16, 2012	Maria Romeo	Maria Romeo	Review of additions to executive summary indicating CBSA will explore audio capture in future
07	Nov. 20, 2012	Darren Okabe	Kory Beecroft	Additions to four-part Oakes test. Separation of Oakes test from Executive Summary
08	Dec. 13, 2012	Darren Okabe	Stephane Martin	Changes based on internal consultation with DGs Dec 7 and ATIP comments Dec 13
08.1	February 18, 2013	Adam Norwick	Lyne Pelletier	Outstanding changes from previous comments
09	February 20, 2013	Darren Okabe	Adam Norwick	Changes to reflect ATIP comments Feb 18
10	May 01, 2013	Darren Okabe	Adam Norwick	Changes to reflect ATIP comments April 22
11	July 18, 2013	Darren Okabe	Marie-Helene Dupont	Changes to reflect comments from ATIP legal July 15
12	October 1, 2013	Darren Okabe	Adam Norwick	Changes to reflect comments from ATIP September 30
13	October 24, 2013	Darren Okabe Monica Rendon Maureen Haley	Adam Norwick	Changes to reflect comments from ATIP October 23 & 30; and the addition of interview room audio, audio-video content
14	November 12, 2013	Darren Okabe	Megan Imrie	Changes to reflect comments from DGO

Table of Contents

EXECUTIVE SUMMARY	6
ABBREVIATIONS AND ACRONYMS	916
DEFINITIONS	1017
SECTION 1 - OVERVIEW AND INITIATION	1148
OAKES TEST	1724
SECTION 2 - RISK AREA IDENTIFICATION AND CATEGORIZATION	2229
Type of Program or Activity	2229
Type of Personal Information Involved and Context	2330
Program or Activity Partners and Private Sector Involvement	2431
Duration of the Program or Activity	2532
Program Population	2633
Technology and Privacy	2734
Personal Information Transmission	2936
Risk Impact to the Institution	3037
Risk Impact to the Individual or Employee	3037
SECTION 3 - ANALYSIS OF PERSONAL INFORMATION ELEMENTS	3239
SECTION 4 - FLOW OF PERSONAL INFORMATION	3643
4.1 Video Data Flow Model - Diagram	3643
Video Data Flow Explanatory Notes	3845
4.1a Audio and Audio-Video Data Flow Model - Diagram	4148
Audio and Audio-Video Data Flow Explanatory Notes	4249
4.2 Example of a Data Flow Model - Table	4350
4.3 Internal Use and Disclosure	4451
4.4 External Use and Disclosure	4451
4.5 Retention / Storage	4552
4.6 Other Possible Considerations	4853
SECTION 5 - PRIVACY COMPLIANCE ANALYSIS	5055
Legal Authority For Collection Of Personal Information	5055
Necessity To Collect Personal Information	5055
Authority For the Collection, Use or Disclosure Of the Social Insurance Number	5156
Direct Collection - Notification and Consent (as appropriate)	5156
Indirect Collection - Consent or Authority Under Sec. 10 of Privacy Regulations	5257
Indirect Collection - Without Notification and Consent	5358
Retention and Disposal of Personal Information	5459
Accuracy Of Personal Information	5560
Use Of Personal Information	5661
Disclosures Directly Related to the Administration of the Program or Activity	5762
Accounting For New Uses or Disclosures Not Reported in Info Source	6065
Safeguards - Statement Of Sensitivity	6166
Safeguards - Threat and Risk Assessment	6166
Safeguards - Administrative, Physical and Technical	6267
Technology and Privacy - Tracking Technologies	6469
Technology and Privacy - Surveillance or Monitoring	6469
Considerations Related to Compliance, Regulatory Investigation, Enforcement	6570
SECTION 6 - SUMMARY OF ANALYSIS AND RECOMMENDATIONS	6873

SECTION 7 - SUPPLEMENTARY DOCUMENTS LIST	6873
SECTION 8 - FORMAL APPROVAL	6974

EXECUTIVE SUMMARY

This PIA has been drafted using the Canada Border Services Agency's (CBSA) *Policy on the Overt Use of Audio-Video Monitoring and Recording Technology* (AV Policy) as well as the associated Directives, the *Privacy Act* and the Privacy Regulations, the *Customs Act (CA)* and the *Immigration Refugee Protection Act (IRPA)* as references. The AV Policy was implemented on August 15, 2011, revised in November 2012 and has since been updated in July 2013 to formalize the deactivation of audio capture except within interview rooms.

Over the past several decades, the CBSA and its predecessors have increasingly implemented the use of Closed Circuit Television (CCTV) technology to carry out its mandate and to ensure the protection of its assets and staff. The use of CCTV cameras to monitor facilities and operations are now an integral part of the CBSA's security framework and operations management.

CCTV cameras are located throughout CBSA operations; they monitor and record CBSA operations at ports of entry (POEs) and inland offices. Areas and activities that may be monitored or recorded include, but are not limited to: Primary Inspection Line (PIL) interviews, secondary examinations, interactions at CBSA information counters, cashier counters, commercial counters, detention cells, and interview rooms. Cameras may also monitor the movement of travellers and goods from one point in a CBSA operation to another, for example, from PIL to secondary.

Audio is only captured in interview rooms during interviews that are conducted for criminal investigations or for the administration of immigration legislation. These interviews may be recorded using audio-only or a combination of audio and video.

Protecting your Personal Information

In order to carry out its mandate, the CBSA must collect a wide variety of personal information. The collection of this information is required in order for CBSA officers to make admissibility decisions regarding persons who wish to enter Canada and goods to be imported into Canada. For the most part, the information collected through the use of CCTV technology is already being collected by the CBSA in one form or another.

All persons who wish to enter Canada are required to provide the following basic personal information: name; citizenship(s); country and place of residence; sex; and must also provide a piece of approved identification, such as a passport or enhanced driver's license. Foreign nationals seeking entry to Canada may also be required to provide the following information: address, or address of destination in Canada; date of birth (age); marital status; employment status; criminal history; fingerprints; and, information related to accompanying goods entering Canada, including purchases made abroad. In all cases, the CBSA collects the personal information deemed necessary to make an admissibility decision.

Through the use of CCTV technologies, the CBSA is also capturing the physical image of the traveller or member of the public, in addition to the other elements of personal information already collected. In the case of a recorded interview, conducted for criminal investigations or for the administration of immigration legislation, the individual's voice is also captured. Within the CBSA, only those employees who require access to video recordings as part of their duties are permitted to do so as per CBSA policies and procedures.

Some personal information collected through overt audio and/or video monitoring and recording activities may be used in support of an investigation regarding national security or criminal activity involving a member of the public or an employee. As a result, audio and/or video recordings may be disclosed to internal stakeholders, such as CBSA Investigations and Inland Enforcement, and external stakeholders, such as the RCMP or CSIS. Recordings may also be used as evidence in criminal proceedings against an individual whose information appears in the recording.

Recordings will not be disclosed for any purpose that is not consistent with the purpose for which the information contained in the recordings was collected or for any purpose that is not consistent with section 107 of the CA where the information is considered to be “customs information,” or with subsection 8(2) of the *Privacy Act* where the information is not considered to be “customs information.”

Any access to or disclosure of video or audio-video recordings must be noted in an audio-video monitoring log. The log entry must include the date and time when the data was accessed, which segment of the data was viewed, by whom and for what reason. Persons who access recordings must identify themselves by name, and badge number if applicable. When a recording is disclosed, the authority for that disclosure must also be noted in the log. Auditing CCTV technologies is not a current practise, however, the audit of access and disclosure is envisioned to be part of the Port Program Assessment process, an integrated review of the current, national CBSA programs.

Retention

Recordings of any video monitoring activity must be retained for no less than thirty (30) days following the date of their creation. Equipment currently in use unable to meet this 30 day minimum requirement is exempt, however any new or replacement CCTV equipment purchased must be capable of storing data for this minimum retention period. Video, audio-video or audio-only recordings that are used by the CBSA (e.g., for evidence or administrative purposes) shall be kept for a minimum of two years following the date of its last use. Since audio recording is only conducted in the context of interviews, where an “administrative purpose” has already been established, the retention period will always be two (2) years following the date of last use.

Right of Access

All recordings, regardless of storage medium, must be stored either in a locked cabinet (or container or a safe) or in a secure room designed in accordance with specifications approved by the Infrastructure and Information Security Division of CBSA.

Recordings will be securely retained in accordance with established policies and guidelines, and may be disclosed both within the CBSA and to our law enforcement partners, and in some cases to Airport or Bridge Authorities responsible for the facilities in which the CBSA operates. Although some Memoranda of Understanding (MOUs) exist to provide for the disclosure of CBSA information to our partners, the CBSA will endeavour to negotiate MOUs with each organization with which the CBSA shares video information.

Individuals may formally request access to your personal information, or access to corporate records related to or created as a result of audio-video recordings by contacting the Access to Information and Privacy Division. More information about this can be found at: <http://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/pia-efvp/atip-airpr/menu-eng.html>. In addition to the requirements specified on the Treasury Board of Canada Secretariat Personal Information Request form, individuals requesting information described by this bank must provide the subject and date of correspondence, incident and location and legal authority for those acting on behalf of an account holder or estate.

Accountability

If individuals have concerns about the collection, use, disclosure or retention of their personal information, they may issue a complaint to CBSA Access to Information and Privacy Division. Complaints should be made in writing, and include their name, contact information, and a brief description of their concerns. Contact information for the Access to Information and Privacy Division at the CBSA can be found here.

<http://cbsa-asfc.gc.ca/agency-agence/reports-rapports/pia-efvp/atip-airp/contact-eng.html>

To make a compliment, comment or complaint, the CBSA has made available a feedback form to help us to understand our clients and improve the delivery of our programs and services. Information on providing feedback can be found here.

<http://www.cbsa-asfc.gc.ca/contact/com-eng.html>

Please note that the CBSA is not currently capturing audio information outside of interview rooms where it is captured with the knowledge and consent of the person providing the statement. While the Agency continues to explore the use of audio, no decision has been made regarding its capture beyond interview rooms. Should the CBSA pursue with the intent of deploying audio technology, a PIA addressing the use of audio will be submitted to your office for your review and recommendations before activating any such equipment.

The CBSA has posted a Video Recording and Monitoring Privacy Notice on their external website November 19, 2012. This Privacy Notice outlines the use of, retention and disposal of and access to CBSA recordings; and includes a link to the PIB described in Info Source below:

<http://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/pia-efvp/atip-airp/infosource-eng.html>

ABBREVIATIONS AND ACRONYMS

The following is a list of abbreviations and acronyms used in this report:

ATIP	Access to Information and Privacy
CA	Customs Act
CBSA	Canada Border Services Agency
CC	Criminal Code
CSIS	Canadian Security Intelligence Service
IRPA	Immigration and Refugee Protection Act
MOU	Memorandum of Understanding
PIB	Personal Information Bank
PIL	Primary Inspection Line
POE	Port of Entry
RCMP	Royal Canadian Mounted Police
TBS	Treasury Board Secretariat

DEFINITIONS

This section provides definitions of the terms frequently used in this report:

Administrative purpose	The <i>Privacy Act</i> defines an “administrative purpose” to be the use of an individual’s personal information in a decision-making process that directly affects that individual.
Consistent use	Is a use that has a reasonable and direct connection to the original purpose(s) for which the information was obtained or compiled. This means that the original purpose and the proposed purpose are so closely related that the individual would expect that the information would be used for the consistent purpose, even if the use is not spelled out.
Customs Information	Means information of any kind and in any form that relates to one or more persons and is obtained by, or on behalf of, (i) the Minister for the purposes of the <i>Customs Act</i> or the <i>Customs Tariff</i> , or (ii) the Minister of National Revenue for the purposes of debts due to Her Majesty under Part V.1 of the <i>Customs Act</i> , or any information that is prepared from the information described above.
Event	As defined in the AV Policy, means any occurrence that may reasonably be expected to require further action by the CBSA or that may reasonably be expected to go to court or to a tribunal and that justifies reviewing video data. An event may include, but is not limited to, the following: arrest of a traveller, national security incidents, assault on or hindering an officer, altercations between members of the public, use of force incidents, discharge of a duty firearm, vehicle searches resulting in enforcement action, verbal complaints, port runners, medical emergencies and environmental catastrophe.
Info Source	Is a series of annual Treasury Board Secretariat publications in which government institutions are required to describe their institutions, program responsibilities and information holdings, including PIBs and classes of personal information. The descriptions are to contain sufficient clarity and detail to facilitate the exercise of the right of access under the <i>Privacy Act</i> . Data-matching activities, use of the SIN and all activities for which privacy impact assessments were conducted have to be cited in <i>Info Source</i> PIBs, as applicable. The <i>Info Source</i> publications also provide contact information for government institutions as well as summaries of court cases and statistics on access requests.
Personal Information Bank	Is a description of personal information that is organized and retrievable by a person's name or by an identifying number, symbol or other particular assigned only to that person. The personal information described in the personal information bank has been used, is being used, or is available for an administrative purpose and is under the control of a government institution.
Transitory Record	As defined by Library and Archives Canada and for the purposes of this policy are those audio-video records that have no enduring value to the CBSA. They are records that are required only for a limited time to ensure the completion of a routine action or the preparation of a subsequent record but do not include records that are required to control, support or document the delivery of programs, to carry out operations, to make decisions, or to account for activities of government. (Source: <i>MIDA 2.1</i> , 4. Definition)
Primary Inspection line	The term "Primary Inspection Line" is used to refer to the point at which the person entering Canada makes a report of his or her person and goods as required under the <i>Customs Act</i> and the IRPA. The CBSA has PIL booths from which officers conduct primary examinations.

SECTION 1 - OVERVIEW AND INITIATION

Government Institution: Canada Border Services Agency

Government Official Responsible for the Privacy
Impact Assessment

Barry Kong, Compliance and Program
Management Director, CBSA

Head of the government institution / Delegate for
section 10 of the *Privacy Act*

Dan Proulx, ATIP Director, CBSA

Name of Program or Activity of the Government Institution:

Use of Overt Video Monitoring and Recording Technology

Description of Program or Activity:

The CBSA uses overt video monitoring and recording technologies in support of existing programs as an integral part of its security framework and its operations management in order to ensure the integrity of the Canadian border. The use of overt video monitoring and recording technologies supports the Enforcement, Facilitated Border, and Conventional Border programs, and increases the CBSA's ability to meet its mandate and its ability to protect the public, its employees and its assets.

Cameras monitor and record CBSA operations at ports of entry and inland offices. Areas and activities that may be monitored or recorded include, but are not limited to: PIL interviews, secondary examinations, interactions at CBSA information counters, cashier counters, commercial counters, detention cells, and interview rooms.

The CBSA captures limited audio information in the execution of its mandate under the *Canada Border Services Agency Act*. Specifically, interviews, which are conducted in the enforcement of the *Customs Act*, the *Immigration Refugee Protection Act* (IRPA) and other CBSA program legislation, may be recorded by audio-only or by video in combination with audio.

Criminal Investigation

An individual who is the subject of, or a witness to, a criminal offence is not obligated to provide information related to that offence; it is provided voluntarily with the individual's consent, otherwise it would not be admissible as evidence.

Before the statement can be admissible as evidence, the court must be satisfied that it was made freely and voluntarily. The rules governing the admissibility of statements (commonly referred to as the "Judges Rules") are applicable to all statements made to a person(s) in authority. A person in authority is generally accepted to mean anyone connected with the arrest, detention, examination or prosecution of the subject or anyone whom the subject believes may influence the case.

To ensure that a statement is considered voluntary, officers must be able to prove to the court that the statement was made without fear or inducement. In this regard, an inducement can be described as anything said or done by

a person in authority, which would lead the subject to believe his position with respect to the charge will be better or worse dependent on the uttering of the statement.

There are no consequences to failing to provide a statement; however, the *Criminal Code* creates offences related to misleading or obstructing justice by making false statements. The individual is made aware of these consequences.

An individual who is subject of an investigation is read the standard caution against making statements and informed that the information they provide may be used as evidence. The standard caution for CBSA officers is provided below although the standard caution used by the police agency of jurisdiction may also be read.

You need not say anything. You have nothing to hope from any promise or favour, or nothing to fear from any threat, whether or not you do say anything. Anything you do say may be used as evidence. Do you understand?

In addition to providing the statement voluntarily, the individual also provides verbal or written consent for their statement to be recorded.

Administration of IRPA

An individual making an application under IRPA, which includes seeking to enter Canada and making a claim for refugee protection, is obligated to provide certain information as part of that application. Failure to provide that information can result in the application being rejected, which could include the individual being found inadmissible to Canada. Persons who knowingly refuse to answer a question put to them at an examination can be charged with an offence under section 127 of IRPA. Individuals are counseled on the consequences of failing to provide information at the commencement of the interview. Notification and verbal consent is obtained at the outset of all audio-recorded interviews. Individuals are also informed of the purpose for which the information they provide will be used.

TARGETING

The Targeting Program identifies people and goods bound for Canada that may pose a threat to the security and safety of the country. The CBSA uses a number of automated advance information sources from carriers and importers to identify people, goods and conveyances that may pose a threat to Canada. Advance Passenger Information and Advance Commercial Information provide the CBSA with electronic pre-arrival information on people and goods that can be used to perform risk assessments in advance of their arrival in Canada. Known threats are identified when there is a match against an enforcement database entry. People and goods that are identified as posing a threat to Canada are referred for verification and examination upon their arrival at a port of entry.

Note: This should align with the program named and described in the institution's Info Source Chapter as required under section 5 of the *Access to Information Act*. For institutions that develop a Program Activity Architecture (PAA) as per the Management, Resources, and Results Structure Policy, the institutional Info Source chapter must align with the programs, activities and sub-activities described in the PAA.

Description of the class of records associated with the program or activity:

CBSA BPD 1101

Records include audio/video footage of CBSA operations including primary inspection line (PIL) interviews; secondary examinations; interactions at CBSA information counters, cashier counters, commercial counters, in detention cells, and in interview rooms to record audio statements made under the Immigration and Refugee Protection Act (IRPA).

Class of Record Number: CBSA BPD 1101

☒ **Proposal for a New Personal Information Bank**

TBS Registration: 20110287

Bank Number: CBSA PPU 1104

Description: This bank describes information that is used in support of audio-video, audio only and video only overt surveillance recordings generated by overt audio-video recording systems at CBSA ports of entry and inland offices. The personal information may include name, contact information, biographical information, citizenship status, gender and criminal checks/history, date of birth, educational information, employment equity information, financial information, medical information, physical attributes and place of birth.

Note: In addition to the requirements specified on the Treasury Board of Canada Secretariat Personal Information Request form, individuals requesting information described by this bank must provide the subject and date of correspondence, incident and location and legal authority for those acting on behalf of an account holder or estate.

Class of Individuals: General public, all non-CBSA employees working in affected areas and all off-duty CBSA employees in accordance with paragraph 3(j) of the *Privacy Act*.

Purpose: The personal information is used to provide services for the overt audio-video surveillance activities. Personal information is collected pursuant to 5(1)(a) of the Canada Border Services Agency Act.

Consistent Uses: The information may be used or disclosed for the following purposes: enforcement, reporting to senior management, safety, security and program evaluation. Audio-video recordings may be shared with Canadian Security Intelligence Service (CSIS), Royal Canadian Mounted Police (RCMP) and other Federal law enforcement Agencies for investigative and enforcement purposes. Audio-video recordings may be shared with provincial law enforcement agencies for the purpose of enforcing federal and/or provincial law. Audio-video recordings may be shared with municipal or regional law enforcement agencies for the purpose of enforcing federal and/or provincial law. Audio-video recordings may be shared with Canada Border Services Agency (CBSA) Investigations and Intelligence to enforce federal and/or provincial law and with Security and Professional Standards to conduct administrative Investigations into employee misconduct.

Privacy Impact Assessment (PIA): The development of a PIA is in progress. The expected completion date is November, 2013.

Retention and Disposal Standards: Recordings of any video monitoring activity must be retained for no less than thirty (30) days following the date of their creation.

Note: This clause does not apply to audio-video technology already in use that is unable to meet this requirement. Any new or replacement audio-video monitoring and recording equipment purchased following the implementation of this policy must be capable of storing data for the minimum retention period.

Recordings that are used to obtain or provide information or to investigate an allegation or complaint, or used as evidence in respect of an identifiable individual shall be kept for the longer of two (2) years following the date of their creation, or following the date of their last use in an administrative action as information or as evidence in respect of that person.

RDA Number: Currently under development.

Related Class of Record Number: CBSA BPD 1101

TBS Registration: 20110287

- Please note that the above PIB is currently under review.

- ☐ Proposed new Standard Personal Information Bank
- ☐ Proposal to modify an existing Standard Personal Information Bank - identify Standard PIB number and current description:

N/A – all records are institution specific.

Legal Authority for Program or Activity:

Canada Border Services Agency Act, paragraph 5(1)(a)

Note: Prior to proceeding with the assessment it is essential that Parliamentary authority for the relevant program or activity be established. Generally, Parliamentary authority is usually contained in an Act of Parliament or subsequent regulations, or approval of expenditures proposed in the Estimates and authorized by an *Appropriations Act*. If legal authority is unclear consult your Legal Service to determine authority for the program or activity. (See question 1 of **Section V**)

Summary of the project / initiative / change:

The CBSA works to promote the free flow of travellers and goods, into and out of Canada, while ensuring that security measures are in place to stop and remove potential threats. Keeping Canada's border open to travel and trade, but closed to criminal activity requires the CBSA to manage border operations effectively.

With a workforce of approximately 14,000 employees, the CBSA provides services at 1,200 points across Canada. The CBSA also administers more than 90 acts, regulations, and international agreements, many on behalf of other federal departments and agencies, the provinces, and the territories. In fiscal year 2011-2012, the CBSA processed 98 million travellers and 13 million commercial shipments.

The CBSA uses overt video monitoring and recording technologies in support of existing programs as an integral part of its security framework and its operations management in order to ensure the integrity of the Canadian border and the health and safety of its employees as well as that of the travelling and Canadian public. The use of overt video monitoring and recording technologies increases the CBSA's ability to meet its mandate and its ability to protect the public, its employees and its assets.

Cameras monitor and record CBSA operations at POEs and inland offices. Areas and activities that may be monitored or recorded include, but are not limited to: PIL interviews, secondary examinations, interactions at CBSA information counters, cashier counters, commercial counters, detention cells, and interview rooms. Cameras may also monitor the movement of travellers and goods from one point in a CBSA operation to another, for example, from PIL to secondary.

Cameras assist the CBSA in ensuring the integrity of the border by capturing information relating to persons who contravene sections 11 and 12 of the *Customs Act* (CA) and section 18 of the *Immigration and Refugee Protection Act* (IRPA) by failing to present themselves and their goods for examination at the border. Cameras help detect threats to the health and safety of CBSA employees and the public, and information captured can be used to assist in the investigation of illegal activity committed in relation to the legislation enforced by the CBSA.

Cameras will not be placed in any area where CBSA business is not conducted, or in any area where there would be a heightened expectation of privacy, such as public or employee washrooms, lunch rooms and locker rooms. Information related to travellers, facility employees (non-CBSA) or other members of the public (transport drivers, flight attendants, brokers clearing goods, etc.) is considered to be personal information as defined in section 3 of the *Privacy Act*. For the purposes of this activity and this PIA, any CBSA employee information captured in video recordings that relates to the function or the position of the employee is not considered to be personal information, in accordance with paragraph 3(j) of the *Privacy*

Act. Any information captured related to an employee that does not specifically relate to his/her function or position will be treated as personal information per section 3 of the *Privacy Act*.

The CBSA recognizes that it has broad authorities to stop, question, search, detain and arrest travellers and seize goods and information in the border context. It further recognizes that, in order to carry out its mandate to ensure the safety and security of the Canadian border, it collects and is entrusted with a wide variety of personal information. The CBSA is committed to adhering to all privacy laws and to ensuring not only that individuals are appropriately notified of any collection of personal information, but that all of the information collected is appropriately protected.

The overt use of video monitoring and recording technology is not a new activity. However, despite the fact that the CBSA is already using this technology, there has been no overarching policy to guide the use of equipment and recordings, or their retention, disclosure and disposal. The CBSA has decided to conduct this PIA in order to ensure that the privacy risks associated with collecting, using, and disclosing personal information in the form of video recordings are adequately addressed.

The information collected through this activity supplements the information that the CBSA is already collecting. The only new information being captured through this activity is a record of the physical images of individuals who interact with the CBSA at service locations. All other information discussed in this PIA is already being collected in one form or another.

When authorized by law, video recordings may be disclosed within the CBSA for various enforcement-related purposes such as the investigation of CA or IRPA offences. Video recordings may also be disclosed outside the CBSA to our law enforcement partners for the purposes of investigation of *Criminal Code* (CC) and other federal offences, as well as for the purposes of prosecution of those offences. In addition, in some cases recordings may be disclosed to private sector organizations such as Airport or Bridge Authorities, when agreements are in place to support lawful information sharing, and only when such sharing is necessary.

This PIA reflects the CBSA's overt use of video monitoring and recording technology at POEs and inland offices across Canada as of August, 2011.

This PIA has been drafted using the AV Policy as well as the associated Directives, the *Privacy Act* and the *Privacy Regulations*, the *Customs Act* and the *Immigration Refugee Protection Act* as references. The AV Policy was implemented on August 15, 2011 and revised in July 2013 to formalize the deactivation of audio capture except within interview rooms and strengthen direction on retention, access and prohibited use for private conversations.

Stakeholders include: local, provincial and federal law enforcement agencies, CBSA Investigations, CBSA Intelligence, CBSA Security and Professional Standards Directorate, Airport and Bridge Authorities where the CBSA operates.

OAKES TEST

The CBSA also offers the following in answer to the four part test regarding video surveillance of public places:

1. Is the measure demonstrably necessary to meet a specific need?

Yes, over the years that the CBSA has used overt video monitoring and recording, it has proven itself demonstrably necessary to support its programs and operations. Specific needs include the safety of CBSA officers and the public in CBSA operational areas, the security of CBSA buildings and equipment, and the evidence to support seizures or prosecutions under the *Customs Act*, the *Immigration and Refugee Protection Act* and the *Criminal Code*.

The Dziekanski incident at Vancouver International Airport (VIA) demonstrated that video recordings were necessary to assist in the initial investigation of the Vancouver Airport Authority, the CBSA and RCMP, and the Braidwood Inquiry which followed. In this inquiry it was noted that video footage of Mr. Dziekanski in the Customs Hall showed “nothing to indicate that he was unsteady on his feet (i.e., that he was ataxic), which is usually the case with cerebellar degeneration.”

This unfortunate incident and the following results of the Braidwood Inquiry brought sweeping changes to the Standard Operating Procedures (SOPs) of airport authorities and the CBSA. Along with the installation of an information booth for travellers, improved language services and more patrols, the CBSA made improvements to the closed-circuit television system to better allow staff to observe the passenger hall. The CBSA hall now has cameras which record 24-hours-a-day. These recommended changes enhance the safety of travelers and officers and the security of CBSA buildings and equipment at VIA as well as at other international airports across the country.

Formal investigations of certain CBSA officers for alleged criminal acts demonstrated that the video monitoring and recording of officer conduct while performing their duties are necessary to ensure a culture of professional integrity amongst its employees. Proper officer conduct directly affects the image of the agency and Canada itself and directly influences the safety, security and overall border experience of travellers.

A recent court case, for example, involving an on duty Border Services Officer at the Port of Douglas in B.C., demonstrates the necessity of video monitoring and recording. In 2007 it was alleged that a male officer brought 4 female travellers offsite to a public washroom or dimly lit fenced area on separate occasions and sexually assaulted 3 of them. Earlier in the trial, a woman testified that she was instructed by the officer to cross a road to a men’s washroom to be strip searched. Video footage was later played in court showing the officer cross the road and immediately after, a woman crossing. The officer explained under oath, that he was likely grabbing a Coca-Cola and batteries from his car. However, video evidence showed that the officer did not have a can of pop with him upon returning to the CBSA building. The Crown called his actions “an appalling abuse of authority” and said the women only agreed to the ordeals under duress. The jury found the officer guilty of 3 counts of sexual assault and 1 count of breach of trust. The video evidence, contrary to the officer’s statements, provided the jury a reasonable doubt that the officer’s testimony was truthful.

2. Is it likely to be effective in meeting that need?

Yes, in addition to meeting the needs stated above, overt video monitoring and recording should encourage compliance with border related legislation, while supporting the safety and security of officers and travellers.

Remote border locations, for example,

depend on CCTV technology to support the security of the border by capturing images of vehicles, license plates and travellers who cross without authority and to increase the safety of officers. CCTV technology aids in the protection and safety of officers not only in these remote locations but helps secure ports of entry across the country. For example, designated telephone reporting sites where no officers are present would benefit from using CCTV technology to supplement the telephone reporting information of persons seeking to enter Canada at marinas or wharfs. Even at large ports of entry, where travellers amount in the millions crossing per year, the CBSA depends of CCTV technology to support officer and traveller safety.

CCTV also protects equipment owned by the CBSA. Server rooms for instance, at times containing thousands of dollars of computer servers and in locations where CCTV is used, digital video recorders containing hundreds of hours of video footage, are in locked rooms. Updated facilities, mostly the newest larger ports have cameras located in these rooms to help keep this equipment secure. CCTV is also used at ports which have secure bond locations (locked rooms or securely gated areas for detained or seized goods) and with the introduction of arming for officers, some ports have dedicated arming rooms to ensure that Agency firearms are safely and securely stored.

Human rights complaints, for example, are vetted through the Human Rights Complaints Commission which evaluates the evidence submitted in discrimination complaints. The Commission requests that officers prepare accurate and complete notes detailing why certain actions were taken during a given incident i.e., referral, personal search, questioning etc. These notes and other documentation, including video surveillance, play a key role in the preparation of submissions to the Commission in defending the CBSA's position.

Even if the Commission is unaware of video surveillance, this evidence may still play a key role in a tribunal's decision. For instance, the existence of video footage of an individual seeking entry to Canada in 2005 was revealed 4 years later at her human rights tribunal in 2009. Her story is that of particularly harsh treatment during an unexplained vehicle scan at the port of entry in Cornwall, ON. The now 8 year old video footage was recently shown at the tribunal in August, and as of September 2013 the hearings continue.

Compliance with border related legislation is not only for the travellers crossing the border. A former Border Services Officer was sentenced in 2012 to 14 years imprisonment for his part in facilitating the smuggling of narcotics by 3 other accomplices. The Crown highlights the level of sophistication involved in the scheme, in particular "(his) actions at the border to wave Johal and Riari through and his pretending not to know either of them." Video evidence in this case was essential in providing the court with the timeline of the event and the relation between officer and travellers, from the time the officer entered the booth, to his personal cellphone use, up to the facilitated crossing of his two accomplices. CCTV technology was used successfully to regain the

public's confidence to enforce the law in an objective manner and keep hundreds of kilograms of cocaine off the street.

3. Is the loss of privacy proportional to the need?

Yes, in fact the loss of privacy is minimal given the lower expectation of privacy in a border crossing context.

The CBSA fulfills its mandate through the administration or enforcement of over 90 Acts and Regulations. As a result the Agency is responsible for numerous and complex programs and operating activities. In addition to contending with the breadth and complexity of its mandate, the CBSA must also deliver these programs on a very large scale. In fiscal year 2012-13, the CBSA provided border-related services for close to 100 million travellers and 14 million commercial releases as well as 36 million courier shipments and 44 million postal shipments arriving at our land, air, rail and marine ports of entry. The CBSA relies on CCTV to help us deliver our programs in the face of these pressures.

Video monitoring and recording only takes place where CBSA business is conducted and to safeguard CBSA buildings and equipment at POEs and inland offices. Personal information already collected at POEs includes a traveller's name; citizenship(s); country and place of residence; sex; and must also provide a piece of approved identification, such as a passport or enhanced driver's license. Persons seeking entry to Canada may also be required to provide the following information: address, or address of destination in Canada; date of birth (age); marital status; employment status; criminal history; fingerprints; and, information related to accompanying goods entering Canada, including purchases made abroad. CCTV technology, in addition to the elements mentioned, also captures the physical image of the traveller which is necessary in identifying individuals involved in CBSA events, whether safety and security related or as evidence to support seizures or prosecutions. In all cases, the CBSA only collects the minimum amount of personal information required to make an admissibility decision or in the case of video, the minimum amount required to identify and if necessary provide evidence for court purposes.

The recent shooting of a Border Services Officer in B.C., objectifies the need for this type of surveillance. The video footage apparently shows that the shooter immediately shot the officer after pulling up in his vehicle to the inspection booth. The officer had no warning and no chance to react. Luckily, the officer survived the attack and was later interviewed by police. However, victims of crime cannot be relied upon to recall the event as it truly happened, as understandably, they have suffered physical and mental trauma and are likely in a state of mental shock. An honest recollection of the event may be incorrect. The video surveillance offers the only true insight as to what actually happened. It can be slowed down, played frame by frame and if need be, digitally enhanced. Eye witness accounts are most likely of events post gunfire, and though any recollection of such events are often enhanced by adrenaline, at the same time this recall may be tainted by emotions, in this case fear, opening up any testimony to scrutiny.

4. Is there a less privacy-invasive way of achieving the same end?

No, overt video monitoring and recording at port of entry locations cannot be achieved by any other less privacy-invasive technology to achieve the same end.

The safety of officers and the public in CBSA operational areas, for example video recordings of Mr. Dziekanski at Vancouver International Airport, could not have been achieved in a less-privacy invasive way. Recordings of Mr. Dziekanski provided invaluable evidence at the Braidwood Inquiry to corroborate the testimony of witnesses in reference to Mr. Dziekanski's location and time of arrival and departure from the hall. Video also provided evidence, again in support of witness testimony, regarding Mr. Dziekanski's possible state of mind during his time in the baggage claim area. With thousands of travellers arriving per day through customs and immigration and the amount of hours that Mr. Dziekanski spent in this area, it seems likely that no amount of physical presence (e.g. supervisors) in the hall could have provided evidence of location and time as accurately as video recordings.

Cameras in designated currency counting areas for example provide an unbiased view of the sometimes large sums of currency being handled by officers enforcing the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA). Officers consider the cameras as a safety net for unfounded complaints from travellers who report currency missing and alternatively, travellers who recognize the CCTV cameras appreciate the added security of their money. When counting currency, enforcement policy recommends this action be in presence of the client and another 'observing' officer. While this recommended procedure is less privacy-invasive, this is not always possible and would not deter allegations from travellers that both officers are corrupt.

The security of CBSA buildings and equipment can be achieved by having a security guard posted in all sensitive areas/buildings, 24 hours a day, 7 days a week. This would be equally as effective as video monitoring; however it may not be as less-privacy invasive. The guard can see and hear more than what is overtly monitored as the camera feed is video only and the view is most likely static. The image may also be low definition and the subject too far away, below the camera or beyond the field of view. Also a guard can move towards a subject and speak with them; asking who they are and what are they doing here etc. Building security video recordings are used successfully as evidence for court purposes as long as the authenticity of the recording is unquestionable.

As stated, recorded evidence for example, which can support seizures or prosecutions in a court of law cannot be achieved in a less-privacy invasive way. The physical image of a person committing alleged actions is undoubtedly hurtful to the case of the accused. Eyewitness testimony has proven to be easier disputed in court¹ and therefore less reliable than today's digital imaging technology.

¹. Laura Engelhardt, "The Problem with Eyewitness Testimony," Stanford Journal of Legal Studies Vol. 1.1 (December 1999): 25-30

The CBSA also offers the following in answer to the four part test regarding the recording of interviews:

Is the measure demonstrably necessary to meet a specific need?

Yes. In the case of either a criminal investigation or an administrative process under IRPA, there is a need to accurately record the information an individual provides during an interview so that it can be used as evidence in the associated proceeding (e.g. court or administrative tribunal, etc.) Recording

the interview, using either audio-only or audio-video recording technology provides the most objective and reliable method for meeting that need.

In the criminal context, the Supreme Court has recognized the benefits of recording interviews as a means of assisting the courts in monitoring interrogation practices and protecting against untrustworthy confessions.¹ The *Youth Criminal Justice Act* codifies this as a requirement with respect to statements made by persons less than 18 years to ensure the statement was provided voluntarily and that the young person understood the impact of waiving his or her right to counsel.²

Even though no penal liability applies in the administrative context under IRPA, it is still important to create an accurate record of a statement to protect the fairness of the administrative process. Information provided in an interview may confirm or disconfirm an individual's admissibility to Canada and may be used as evidence in decisions made by the Minister's Delegate, Immigration Division, Refugee Protection Division and possibly the Federal and Supreme Courts of Canada should the decision be appealed.

Is it likely to be effective in meeting that need?

Yes. Recorded interviews provide an accurate and objective record of the information provided during the interview and the interaction between the individual and the officer that is easily reviewed by the courts or other relevant decision-maker.

Is the loss of privacy proportional to the need?

Yes. The intrusion on privacy is not significant greater than it would be with the traditional practice of conducting an interview with the officer taking detailed notes. More information is captured during a recorded interview (e.g. tone of voice, image of the officer and individual, body language, etc.) but this information is important to establishing an objective record. These aspects provide the court or other administrative decision-maker with useful information in considering the admissibility of the statement, the conduct of the officer, the context of a given statement, etcetera.

In this respect, the practice of recording an interview protects both the investigating agency and the individual being interviewed.

Is there a less privacy-invasive way of achieving the same end?

No. Many interviews are not recorded and the officer makes detailed notes to provide a record. This is effective in capturing the significant content of the interview but is not as effective in providing a complete and objective record of the interaction.

¹ *R. v. Oickle*, 2000 SCC 38, [2000] 2 S.C.R. 3

² *Youth Criminal Justice Act* s. 146(4)(a) and (b)

SECTION 2 - RISK AREA IDENTIFICATION AND CATEGORIZATION

For Section 2, please check the appropriate box that describes the level of risk related to your program or activity and provide details as indicated in yellow.

Type of Program or Activity	Level of Risk
Program or activity that does NOT involve a decision about an identifiable individual Personal information is used strictly for statistical / research or evaluations including mailing list where no decisions are made that directly have an impact on an identifiable individual. The Directive on PIA applies to administrative use of personal information. The Policy on Privacy Protection requires that government institutions establish an institutional Privacy Protocol for addressing non-administrative uses of personal information.	<input type="checkbox"/> 1
Administration of Programs / Activity and Services Personal information is used to make decisions that directly affect the individual (i.e. determining eligibility for programs including authentication for accessing programs/services, administering program payments, overpayments, or support to clients, issuing or denial of permits/licenses, processing appeals, etc...).	<input type="checkbox"/> 2
Compliance / Regulatory investigations and enforcement Personal information is used for purposes of detecting fraud or investigating possible abuses within programs where the consequences are administrative in nature (i.e., a fine, discontinuation of benefits, audit of personal income tax file or deportation in cases where national security and/or criminal enforcement is not an issue).	<input type="checkbox"/> 3
Criminal investigation and enforcement / National Security Personal information is used for investigations and enforcement in a criminal context (i.e. decisions may lead to criminal charges/sanctions or deportation for reasons of national security or criminal enforcement).	<input checked="" type="checkbox"/> 4
Details: Some personal information collected through overt video monitoring and recording activities may be used in support of an investigation into criminal activity or a matter pertaining to national security involving a member of the public or an employee.	
Video recordings (including audio and/or audio-video in interview rooms) may be disclosed to internal stakeholders, such as CBSA Investigations, Inland Enforcement, and external stakeholders, such as the Royal Canadian Mounted Police (RCMP) and the Canadian Security Intelligence Service (CSIS), and local and municipal law enforcement agencies for the purposes of criminal or national security investigations. Video recordings may be used as evidence in criminal proceedings against an individual whose information appears in the recording.	
Privacy risk: Some personal information collected through overt video monitoring and recording activities (including audio and/or audio-video in interview rooms) may be used in support of an investigation regarding national security or criminal activity involving a member of the public or an employee. As a result, recordings may be disclosed to internal stakeholders, such as CBSA Investigations and Inland Enforcement, and external stakeholders, such as the RCMP or CSIS, for the purposes of criminal investigation or national security. Recordings may also be used as evidence in criminal proceedings against an individual whose information appears in the recording.	
Mitigation: Recordings will not be disclosed for any purpose that is not consistent with the purpose for which the	

information contained in the recordings was collected or if it is not authorized under section 107 of the *Customs Act* when the personal information is “customs information,” or with subsection 8(2) of the *Privacy Act* when the personal information is not considered to be “customs information.” In some cases video recordings owned by the CBSA may be disclosed to private sector organizations such as Airport or Bridge Authorities, when agreements are in place to support lawful information sharing, and only when such sharing is necessary (does not include audio and/or audio-video in interview rooms).

Recordings will only be disclosed in accordance with all relevant legislation and policy.

Type of Personal Information Involved and Context	Level of Risk
Only personal information, with no contextual sensitivities, collected directly from the individual or provided with the consent of the individual for disclosure under an authorized program.	<input type="checkbox"/> 1
Personal information, with no contextual sensitivities after the time of collection, provided by the individual with consent to also use personal information held by another source.	<input type="checkbox"/> 2
Social Insurance Number, medical, financial or other sensitive personal information and/or the context surrounding the personal information is sensitive. Personal information of minors or incompetent individuals or involving a representative acting on behalf of the individual.	<input type="checkbox"/> 3
Sensitive personal information, including detailed profiles, allegations or suspicions, bodily samples and/or the context surrounding the personal information is particularly sensitive.	<input checked="" type="checkbox"/> 4
<p>Details:</p> <p>The CBSA collects a wide variety of personal information in order to carry out its mandate. In order to determine the admissibility of travellers and/or their goods, the CBSA may collect such detailed personal information as occupation, annual salary, sexual orientation, marital status, criminal history, and past drug use. This information may also be captured in video recordings (including audio and/or audio-video in interview rooms).</p> <p>Privacy risk:</p> <p>The CBSA collects a wide variety of personal information through its activities. Video recordings (including audio and/or audio-video in interview rooms) may contain detailed personal information such as occupation, annual salary, sexual orientation, criminal history, and past drug use.</p> <p>Mitigation:</p> <p>The CBSA will collect only the personal information necessary to effectively carry out its mandate.</p> <p>Although some video recordings may be considered to be Protected A (for instance, video recordings of a public area such as the baggage hall where personal information is minimally captured and no audio is captured), the majority of recordings are Protected B (such as interviews at the Primary Inspection Line (PIL) or examinations in the Secondary area) as the information contained in them concerns multiple persons, and each person’s information is generally of a detailed personal nature. As such, all recordings, regardless of storage medium, must be stored either in a locked cabinet (or container or a safe) or in a secure room designed in accordance with specifications approved by the Infrastructure and Information Security Division of CBSA.</p> <p>All retention and disposal of video recordings will be carried out in accordance with the relevant provisions of</p>	

the AV Policy. Disclosure to third parties will be made by the Region or District where the footage is captured. Such disclosure will be made in accordance with section 107 of the *Customs Act* and section 8 of the *Privacy Act*.

The retention period for recordings having no enduring value to the Agency will be 30 days. For all recordings of events requiring further action on the part of the CBSA or that may be required for court, the CBSA has established a minimum two-year retention period in accordance with paragraph 4(1)(a) of the *Privacy Regulations*. In addition, if an ATIP request or formal complaint is received within 30 days of the creation of a recording, that recording will also become subject to the minimum two-year retention period.

Since audio recording is only conducted in the context of interviews, where an “administrative purpose” has already been established, the retention period will always be two (2) years following the date of last use.

The AV Policy:

- All disclosure of audio-video records must be made in accordance with the provisions of the *Customs Act*, the *Access to Information Act*, the *Privacy Act* and/or CBSA disclosure policy.
- When an audio-video record is disclosed in response to an ATIP request from an individual whose information is contained in the record, the identity and other personal information of other individuals in the audio-video record who are not implicated in the request will be protected. If the personal information of a third party cannot be protected, and consent has not been provided for its disclosure, the audio-video record will not be disclosed.

Program or Activity Partners and Private Sector Involvement	Level of Risk
Within the institution (amongst one or more programs within the same institution)	<input type="checkbox"/> 1
With other federal institutions	<input type="checkbox"/> 2
With other or a combination of federal/ provincial and/or municipal government(s)	<input type="checkbox"/> 3
Private sector organizations or international organizations or foreign governments	<input checked="" type="checkbox"/> 4

Details: Audio-video recordings may be disclosed to other government departments and / or law enforcement agencies to further investigations related to criminal activity and / or national security.

Privacy risk:
 Audio-video recordings may be disclosed to other government departments and / or law enforcement agencies to further criminal investigations and with Airport or Bridge or other competent authorities when the situation warrants such sharing.

Mitigation:
 The AV Policy states:

- All disclosure of audio-video records must be made in accordance with the provisions of the *Customs Act*, the *Access to Information Act*, the *Privacy Act* and/or CBSA disclosure policy.
- In addition, the Directives on the Overt Use of Audio-Video Monitoring and Recording Technology state

that:

- Any access to or disclosure of audio-video recordings must be noted in an audio-video monitoring log. The log entry must include the date and time when the data was accessed, which segment of the data was viewed, by whom and for what reason. Persons who access recordings must identify themselves by name and badge number if applicable. When a recording is disclosed, the authority for that disclosure must also be noted in the log.
- When audio-video recordings are copied or extracted in order to be disclosed within the CBSA or to other government departments or law enforcement organizations, the CD, DVD or storage device must be stored in locked storage according to the security classification of the information contained in the audio-video recording. Generally, audio-video recordings are to be classified Protected B.
- Audio-video recordings, including records to be disclosed to other law enforcement agencies and government bodies, may only be disclosed as authorized by the *Privacy Act*, s. 8, *Customs Act*, s. 107, and CBSA disclosure policy.
- Only the segment of the audio-video recording related to the request will be provided. Any unrelated data will be blacked-out, blurred, or obscured by a technique certified as tamper-proof by a credible certification body.
- When audio-video recordings are disclosed for use in legal proceedings, copies shall be made in accordance with the principles concerning the collection of evidence and shall be the record in its entirety. Such disclosure must be noted in the audio-video monitoring log, including the authority for disclosure.
- When other law enforcement organizations are granted access to view and/or copy audio-video recordings, the information regarding this access must be entered in the audio-video monitoring log. The log entry must include which segment of the data has been listened to and/or viewed, by whom, for what reason and indicate whether the other law enforcement agency was provided with a copy of the recording.

Duration of the Program or Activity	Level of risk
One time program or activity Typically involves offering a one-time support measure in the form of a grant payment as a social support mechanism.	<input type="checkbox"/> 1
Short-term program A program or an activity that supports a short-term goal with an established "sunset" date.	<input type="checkbox"/> 2
Long-term program Existing program that has been modified or is established with no clear "sunset".	<input checked="" type="checkbox"/> 3
Details: The CBSA uses overt video monitoring and recording technology as an integral part of its operations and security framework. The use of overt video monitoring and recording technology increases the CBSA's ability to deliver its mandate and protect the public, its employees and its assets.	
Privacy Risk:	

The CBSA collects personal information through video monitoring and activities. These activities will not cease at any time in the future.

Other risks include varying retention periods and capabilities among different technologies within the institution.

Mitigation:

The CBSA will only retain personal information for the minimum amount of time necessary to ensure it is of no enduring value to the Agency or will not be required as evidence of an event that will necessitate further action on the part of the CBSA or for court purposes.

In order to balance the privacy rights of individuals with the needs of the CBSA to ensure the safety and security of Canada, it has been established that the minimum retention period for recordings having no enduring value to the Agency will be 30 days. For all recordings of events requiring further action on the part of the CBSA or that may be required for court, the CBSA has established a minimum two-year retention period in accordance with paragraph 4(1)(a) of the *Privacy Regulations*. In addition, if an ATIP request or formal complaint is received within 30 days of the creation of a recording, that recording will also become subject to the minimum two-year retention period.

Since audio recording is only conducted in the context of interviews, where an “administrative purpose” has already been established, the retention period will always be two (2) years following the date of last use.

It is CBSA’s goal to standardize national CCTV technology that will meet CBSA business needs in the delivery its mandate.

Program Population	Level of Risk
The program affects certain employees for internal administrative purposes.	<input type="checkbox"/> 1
The program affects all employees for internal administrative purposes.	<input type="checkbox"/> 2
The program affects certain individuals for external administrative purposes.	<input checked="" type="checkbox"/> 3
The program affects all individuals for external administrative purposes.	<input type="checkbox"/> 4
Details: Some information collected will be disclosed within the CBSA and to other federal institutions and law enforcement agencies for the purpose of pursuing a criminal investigation. These investigations may lead to prosecution.	
Privacy Risk: Video recordings (including audio and/or audio-video in interview rooms) of interactions with the CBSA may be disclosed to other government departments and law enforcement agencies for the purposes of furthering an investigation or for the purposes of criminal prosecution.	
Mitigation: The CBSA will ensure that any disclosure of video recordings is made in accordance with the relevant policies and legislation. In addition, the CBSA will take steps to ensure that recordings are not disclosed by third parties without the consent of the CBSA. In some cases recordings (does not include audio and/or audio-video in interview rooms) owned by the CBSA may be disclosed to private sector organizations such as airport or bridge authorities, when agreements are in place to support lawful information sharing, and only when such sharing is	

necessary. The CBSA will also endeavour to enter into MOUs with airport and bridge authorities that own and operate CCTV equipment within CBSA areas in order to regularize the disclosure and sharing of authority owned information shared with the CBSA.

Technology and Privacy	
6.1 Does the new or modified program or activity involve the implementation of a new electronic system, software or application program including collaborative software (or groupware) that is implemented to support the program or activity in terms of the creation, collection or handling of personal information?	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO
6.2. Does the new or modified program or activity require any modifications to IT legacy systems and / or services?	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO
6.3 Does the new or modified program or activity involve the implementation of one or more of the following technologies:	
6.3.1 Enhanced identification methods: This includes biometric technology (i.e. facial recognition, gait analysis, iris scan, fingerprint analysis, voice print, radio frequency identification (RFID), etc...) as well as easy pass technology, new identification cards including magnetic stripe cards, "smart cards" (i.e. identification cards that are embedded with either an antenna or a contact pad that is connected to a microprocessor and a memory chip or only a memory chip with non-programmable logic). Please specify: <div style="border: 1px solid black; height: 20px; width: 100%;"></div>	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO
6.3.2 Use of Surveillance: This includes surveillance technologies such as audio/video recording devices, thermal imaging, recognition devices, RFID, surreptitious surveillance / interception, computer aided monitoring including audit trails, satellite surveillance etc. Please specify: <div style="border: 1px solid black; padding: 5px;"> <p>The CBSA uses overt video monitoring and recording technologies to monitor and record CBSA operations at ports of entry and inland offices. Areas and activities that may be monitored or recorded include, but are not limited to: primary inspection line (PIL) interviews, secondary examinations, interactions at CBSA information counters, cashier counters, commercial counters, detention cells, and interview rooms.</p> <p>All persons present in these areas will be subject to monitoring and/or recording.</p> <p>The CBSA captures limited audio information in interview rooms, which are conducted in the enforcement of the <i>Customs Act</i>, the <i>Immigration Refugee Protection Act</i> (IRPA) and other CBSA program legislation, which may be recorded by audio-only or by video in combination with audio.</p> </div>	<input checked="" type="checkbox"/> YES <input type="checkbox"/> NO
6.3.3 Use of automated personal information analysis, personal information matching and knowledge discovery techniques: For the purposes of the Directive on PIA, government institutions are to identify those activities	<input type="checkbox"/> YES <input checked="" type="checkbox"/> NO

that involve the use of automated technology to analyze, create, compare, cull, identify or extract personal information elements. Such activities would include personal information matching, record linkage, personal information mining, personal information comparison, knowledge discovery, information filtering or analysis. Such activities involve some form of artificial intelligence and/or machine learning to uncover knowledge (intelligence), trends/patterns or to predict behaviour.

Please specify:

A **YES** response to any of the above indicates the potential for privacy concerns and risks that will need to be considered and if necessary mitigated.

6.1 Implementation of new cameras

Privacy Risk:

The CBSA has implemented cameras that have the capability to capture audio recordings of any and all individuals found in an area where overt video recording takes place.

Mitigation:

All audio capabilities of these cameras have been disabled, de-activated or removed outside of interview rooms where it is only activated following full disclosure of the intent to record and individuals are read a legal caution concerning any statements made (and if necessary, a secondary caution) informing clients of their right to silence and right against self-crimination.

Caution: "You need not say anything. You have nothing to hope from any promise or favour, or nothing to fear from any threat, whether or not you do say anything. Anything you do say may be used in evidence. Do you understand?"

Secondary Caution: "If you have spoken to any police officer or to anyone with authority, or if any such person has spoken to you in connection with this case, I want it clearly understood that I do not want it to influence you in making any statement. Do you understand?"

The CBSA recognizes and understands that audio capacity de-activated may be accidentally switched on; however the CBSA believes that permanently disabling this capacity would be premature until the CBSA researches and investigates the need for audio capture in other areas outside of interview rooms. Until then, the CBSA will follow direction from the Minister's Office, in which the use of _____ has been accepted as a satisfactory method of de-activating audio. The CBSA also recognizes that permanently disabling the audio capacity may void any warranty on existing equipment and as a result, put more pressure on funding for CCTV technology.

Audio information which is inadvertently captured in a manner inconsistent with the AV policy cannot be used by the CBSA and must be destroyed. Details of this incident must be sent to Programs Branch via the AV Policy Inbox: CBSA-ASFC_AV_Policy-Politique_AV

6.3.2 Use of Surveillance

Privacy Risk:

The CBSA will capture video recordings of any and all individuals found in an area where overt video recording takes place.

Mitigation:

Any recording that is of no enduring value to the Agency, or that does not contain an event that is likely to require further action on the part of the CBSA or that can reasonably be expected to go to court will be disposed of following a minimum retention period of 30 days. Equipment currently in use unable to meet this minimum requirement is exempt, however any new or replacement CCTV equipment purchased must be capable of storing data for this minimum retention period. Recordings that are used by the CBSA (e.g., for evidence) shall be kept for a minimum of two years following the date of its last use.

This minimum retention period of 30 days is intended to balance the needs of the CBSA with the privacy concerns of the individuals whose information is contained in the recordings. The AV Policy provides that any recording that can be disposed of following the minimum 30-day retention period must be disposed of within 15 days of the expiration of that period.

This minimum retention period of two years is in accordance to section 4.1 of the Privacy Regulations.

Event – means any occurrence that may reasonably be expected to require further action by the CBSA or that may reasonably be expected to go to court and that justifies reviewing audio-video data. An event may include, without being restricted to, the following: arrest of a traveller, national security incidents, assault on or hindering an officer, altercations between members of the public, use of force incidents, discharge of a duty firearm, vehicle searches resulting in enforcement action, verbal complaints, port runners, medical emergencies and environmental catastrophe.

Since audio recording is only conducted in the context of interviews, where an “administrative purpose” has already been established, the retention period will always be two (2) years following the date of last use.

Personal Information Transmission	Level of Risk
The personal information is used within a closed system. No connections to Internet, Intranet or any other system. Circulation of hardcopy documents is controlled.	<input type="checkbox"/> 1
The personal information is used in system that has connections to at least one other system.	<input type="checkbox"/> 2
The personal information is transferred to a portable device or is printed. USB key, diskette, laptop computer, any transfer of the personal information to a different medium.	<input type="checkbox"/> 3
The personal information is transmitted using wireless technologies.	<input checked="" type="checkbox"/> 4
Details: Recordings may be transferred from their original recording medium to USB keys, DVDs, etc for storage or for disclosure. Some data may be transmitted wirelessly from the camera to the recording medium, such as a server.	
Privacy Risk: The personal information being transmitted on a wireless network may be compromised. Wireless networks may be necessary in situations where a physically wired connection is impossible due to distance, geography or climate conditions e.g. remote areas in the Yukon or frozen tundra locations in the Arctic.	
Mitigation: The CBSA will ensure that all wireless transmission of data is secure using appropriate technologies. Any transmission of recordings over wireless networks must be done in accordance with the CBSA's Policy on the Use of Wireless Technologies. Wireless transmission of data not in compliance with these protocols must cease	

immediately and the wireless transmission can only resume when authorized by local IT and an official of the Physical Security Section of the Security and Professional Standards Directorate. A Threat Risk Assessment (TRA) of CBSA's audio-video technologies was completed in September 2013 and a summary of this assessment is attached.

Risk Impact to the Institution	Level of Risk
Managerial harm. Processes must be reviewed, tools must be changed, change in provider / partner.	<input type="checkbox"/> 1
Organizational harm. Changes to the organizational structure, changes to the organizations decision-making structure, changes to the distribution of responsibilities and accountabilities, changes to the program activity architecture, departure of employees, reallocation of HR resources.	<input type="checkbox"/> 2
Financial harm. Lawsuit, additional moneys required reallocation of financial resources.	<input type="checkbox"/> 3
Reputation harm, embarrassment, loss of credibility. Decreased confidence by the public, elected officials under the spotlight, institution strategic outcome compromised, government priority compromised, impact on the Government of Canada Outcome areas.	<input checked="" type="checkbox"/> 4
Details: If the recordings are compromised or otherwise released without authority to do so, there is the risk that the information may harm the reputation of the CBSA. As the records contain not only the personal information of travellers and the public, but also serve as a record of how the CBSA does business, inadvertent release of information could cause the public to have decreased confidence in the ability of the CBSA to protect the border.	
Privacy Risk: Should recordings be inadvertently or inappropriately released, an individual may suffer harm to his/her reputation or embarrassment due to the sensitivities surrounding the type of information that can be collected by the CBSA.	
Mitigation: The CBSA will take steps as recommended in the accompanying Threat Risk Assessment Summary to ensure that disclosure of recordings is only made in accordance with the relevant legislation as indicated above. Only those employees who require access to recordings as part of their official duties and who have a need to view them will be permitted to access them. Such permission will be granted in writing and all access to recordings will be monitored by way of access logs. – See Appendices for Privacy Breach Protocol	

Risk Impact to the Individual or Employee	Level of Risk
Inconvenience.	<input type="checkbox"/> 1
Reputation harm, embarrassment.	<input type="checkbox"/> 2
Financial harm.	<input checked="" type="checkbox"/> 3
Physical harm.	<input type="checkbox"/> 4
Details: The inadvertent disclosure of such information without authorization or to an improper party may lead to financial harm, but it is more likely that should the information be compromised it would lead to harm to	

reputation and/or embarrassment. For example, details surrounding an individual's travel including travel companions and their relationship, contents of baggage/vehicle, and responses to questions regarding such topics as criminal history and past drug use may be contained in recordings.

Privacy Risk:

Should recordings be inadvertently or inappropriately released, there is a risk that individuals whose information is contained in those recordings could sue the CBSA given the sensitivities surrounding the information that is collected and the potential impact the release could have on those individuals.

Mitigation:

As above, the CBSA will take steps to ensure that disclosure of recordings is only made in accordance with the relevant legislation as indicated above. Only those employees with a minimum SECRET security clearance who require access to recordings as part of their official duties and who have a need to view them will be permitted to access them. Such permission will be granted in writing and all access to recordings will be monitored by way of access logs.

SECTION 3 - ANALYSIS OF PERSONAL INFORMATION ELEMENTS

Personal Information Elements and Sub-elements

Note: Identification of sub-elements is necessary where sensitive personal information is being collected or where the type of program or activity presents a potential privacy risk at level 2-3-4 in “Section II - Risk Identification and Categorization” of the PIA.

Category Of Personal Information	Personal Information Element	Personal Information Sub-Element	Format	Purpose / Necessity of Element
Gender, physical attributes	Physical image of traveller or other member of the public when video is captured.	<p>At PIL:</p> <ul style="list-style-type: none"> includes a person’s race, national or ethnic origin, religion, or colour; can include information related to travelling companions, including indicators of marital status; can include information related to a person’s employment at a land border, can also include an image of the vehicle that a person is travelling in, including the license plate; <p>At secondary inspection:</p> <ul style="list-style-type: none"> includes a person’s race, national or ethnic origin, religion, or colour; can include information related to travelling companions, including indicators of marital status; can include indicators of employment history and of financial transactions, including information on personal 	Visual Image Recording	<p>To identify clients.</p> <p>To make admissibility decisions regarding the entry of persons and goods to Canada.</p> <p>To ensure the integrity of the border.</p> <p>To ensure the security and health and safety of CBSA employees and members of the public.</p> <p>To ensure the integrity and quality assurance of CBSA programs.</p>

		<p>belongings that may provide information on the person's economic status;</p> <ul style="list-style-type: none"> can include evidence of wrongdoing, such as assault, hindering and officer, or smuggling. <p>At inland CBSA offices:</p> <ul style="list-style-type: none"> includes a person's race, national or ethnic origin, or colour; can include information related to a person's employment (e.g. at a commercial counter, it may be identifiable that a person works for a particular trucking company) 		
Citizenship status, gender, physical attributes	Physical image of a traveller with video recording of primary interview or secondary examination at an airport.	<p>At PIL, video recordings can include:</p> <ul style="list-style-type: none"> a person's race, national or ethnic origin, religion, or colour; information related to travelling companions, including indicators of marital status; <p>At secondary inspection, video recordings can include:</p> <ul style="list-style-type: none"> a person's race, national or ethnic origin, religion, or colour; information related to travelling companions, including indicators of marital status; information on personal belongings that may provide information on the person's economic status; 	Visual Image Recording	<p>To identify clients.</p> <p>To ensure the integrity of the border.</p> <p>To ensure the security and health and safety of CBSA employees and members of the public.</p> <p>To ensure the integrity and quality assurance of CBSA programs.</p>

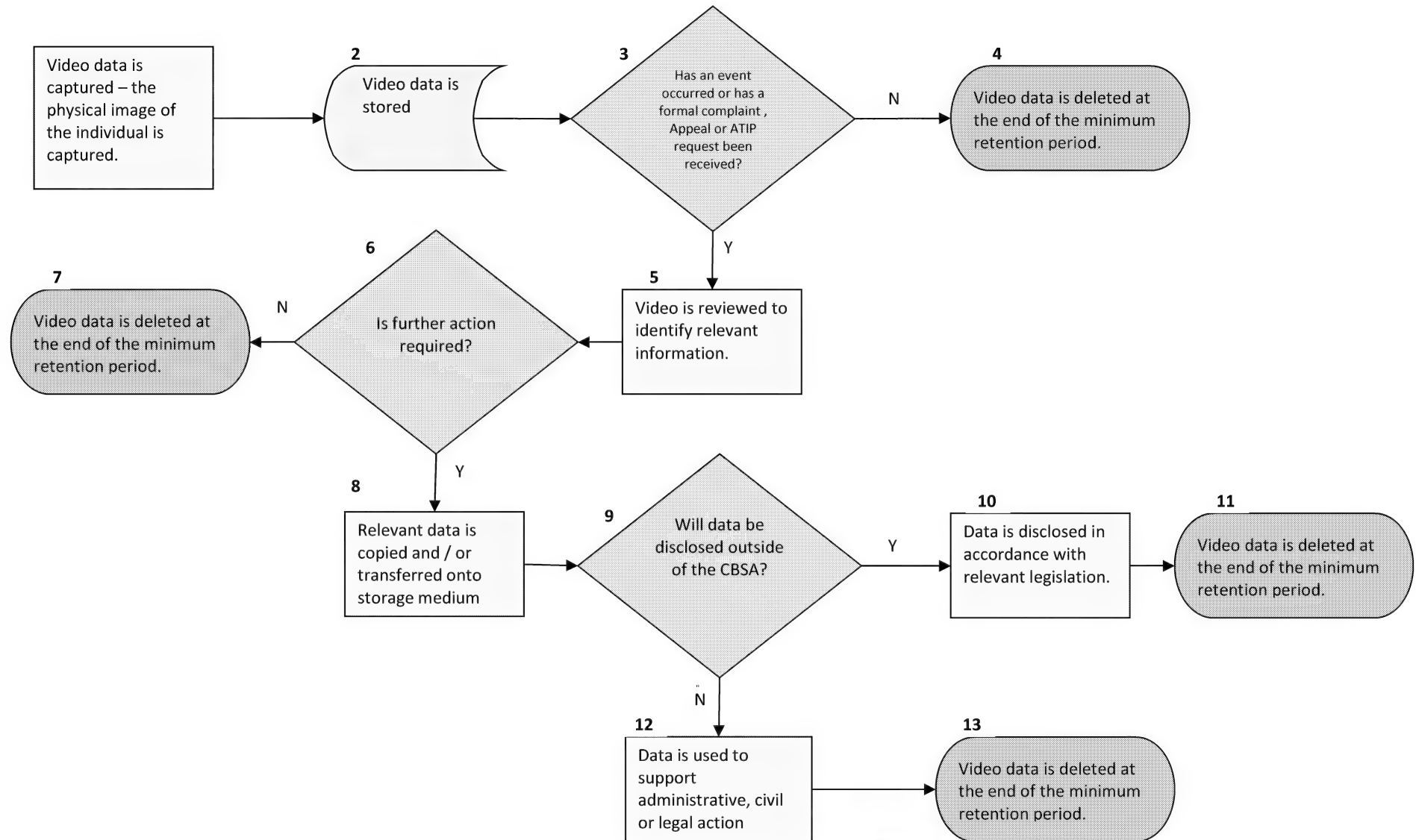
		<ul style="list-style-type: none"> evidence of wrongdoing, such as assault, hindering an officer, or smuggling; 		
Citizenship status, gender, physical attributes	Physical image of a traveller with video recording of primary interview or secondary examination at a land border.	<p>In addition to the personal information indicated above that is captured at an airport, at a land border, the following information may also be captured in video recordings:</p> <p>At PIL:</p> <ul style="list-style-type: none"> an image of the vehicle, including an image of the license plate; a traveller's citizenship; <p>At secondary inspection:</p> <ul style="list-style-type: none"> images of the interior of a vehicle, including the personal belongings of a traveller, which may provide indicators of economic status; <p>Adjacent to the port of entry:</p> <ul style="list-style-type: none"> Cameras may capture images of surrounding areas, which may include images of vehicles, including images of license plates, of vehicles travelling in the area adjacent to the port of entry. 	Visual Image Recording	<p>To identify clients.</p> <p>To ensure the integrity of the border.</p> <p>To ensure the security and health and safety of CBSA employees and members of the public.</p> <p>To ensure the integrity and quality assurance of CBSA programs.</p>
Gender, physical attributes	Physical image of a member of the public with video recording of transaction between that person and the CBSA at an inland service point or	<ul style="list-style-type: none"> Video can include a person's race, national or ethnic origin, religion, or colour; Video can include information related to a person's employment (e.g. at a commercial counter, it may be 	Visual Image Recording	<p>To identify clients.</p> <p>To ensure the integrity of the border.</p> <p>To ensure the security and health and safety of CBSA employees and members of the public.</p> <p>To ensure the integrity and quality assurance of CBSA programs.</p>

	commercial counter.	identifiable that a person works for a particular trucking company)		
Gender, physical attributes,	Physical image of a person under arrest or detention who has been placed in a CBSA detention cell at a port of entry.	<p>The primary purpose for these cameras is to ensure the health and safety of persons held in the cells and CBSA employees. Persons may be held for up to 24 hours.</p> <p>The video may capture:</p> <ul style="list-style-type: none"> • a person's race, national or ethnic origin, religion, or colour; • the fact that a person is held in a cell, which means that the person is suspected of having committed, or has been arrested for, a contravention of the <i>Customs Act</i>, the <i>Criminal Code</i>, or any other Act of Parliament. 	Visual Image Recording	<p>To identify clients.</p> <p>To ensure the integrity of the border.</p> <p>To ensure the security and health and safety of CBSA employees and members of the public.</p> <p>To ensure the integrity and quality assurance of CBSA programs.</p>
Name, date of birth, citizenship as well as details concerning personal life, employment history, criminal history, family life, financial status, personal affiliations, etc.	Voluntary statements made in interview rooms by persons who are under investigation, detention or arrest.	The primary purpose of audio capture in interview rooms is to provide evidence regarding offences relating to the acts and regulations that the CBSA governs at POEs	Audio or audio-video recordings	The CBSA captures limited audio information in the execution of its mandate under the <i>Canada Border Services Agency Act</i> . Specifically, interviews, which are conducted in the enforcement of the <i>Customs Act</i> , the <i>Immigration Refugee Protection Act</i> (IRPA) and other CBSA program legislation, may be recorded by audio-only or by video in combination with audio.

SECTION 4 - FLOW OF PERSONAL INFORMATION

Identify the flow of the personal information within and outside the institution’s program or activity. Institutions may choose to outline the flow of personal information in the format of their choice.

4.1 Video Data Flow Model - Diagram



Video Data Flow Explanatory Notes

1. Video data is captured by means of cameras that are plainly and clearly announced and/or are visible in their placement or use. Signs informing travellers and/or employees that an area is under surveillance have been posted. Cameras may be located in any areas where the CBSA processes persons and goods, or secure areas such as server, arming or currency counting rooms.

Video data is captured for the following purposes:

- (a) To carry out the mandate of the CBSA.
 - (i) To detect and identify persons who fail to present themselves and their goods in accordance with sections 11 and/or 12 of the *Customs Act* and/or section 18 of the *Immigration and Refugee Protection Act* ;
 - (ii) To detect or deter persons who may pose a risk to the health and safety of CBSA employees and members of the public;
 - (iii) To gather information regarding unlawful activity related to any of the legislation enforced by the CBSA e.g. evidence that goods have been unlawfully removed from CBSA control;
 - (b) For the security and protection of CBSA infrastructure including buildings, assets and equipment;
 - (c) For the security and protection or the health and safety of CBSA employees and/or members of the public working in or having access to CBSA owned or operated facilities including ports of entry or any other CBSA office.
 - (d) For purposes related to the integrity and quality assurance of CBSA programs.
2. All video recordings are securely stored as per CBSA policies on the storage of protected information when they are not in use. (Refer to Appendix: Comptrollership Manual – Security Volume – Chapter 6: Storage of Sensitive Information and Assets).

Access to and control of any equipment used for recording purposes is limited to qualified operators who are authorized to do so by the manager responsible for the facility in which the equipment is located. Authorization is provided in writing and specifies the purposes for which access and or control is given.

3. **Event** – means any occurrence that is likely to require further action by the CBSA or that may reasonably be expected to go to court and that justifies reviewing video data. An event may include, without being restricted to, the following: arrest of a traveller, national security incidents, assault on or hindering an officer, altercations between members of the public, use of force incidents, discharge of a duty firearm, vehicle searches resulting in enforcement action, verbal complaints, port runners, medical emergencies and environmental catastrophe.

ATIP Request – A request for information made under the access to information and privacy legislation.

Formal Complaint – A formal complaint includes but is not limited to, a written complaint regarding officer conduct or service received.

4. **Transitory Record** – as defined by Library and Archives Canada and for the purposes of this program are those video records that have no enduring value to the Agency. They are records that are required only for a limited time to ensure the completion of a routine action or the preparation of a subsequent record but **do not** include records that are required to control, support or document the delivery of programs, to carry out operations, to make decisions, or to account for activities of government. (Source: **MIDA 2.1**, 4. Definition)

Recordings that are considered to be transitory records will not be disclosed outside or within the CBSA and will be deleted/disposed of following the expiration of the minimum 30-day retention period for transitory records.

Operational Record – records that are required to control, support or document the delivery of programs, to carry out operations, to make decisions, or to account for activities of government.

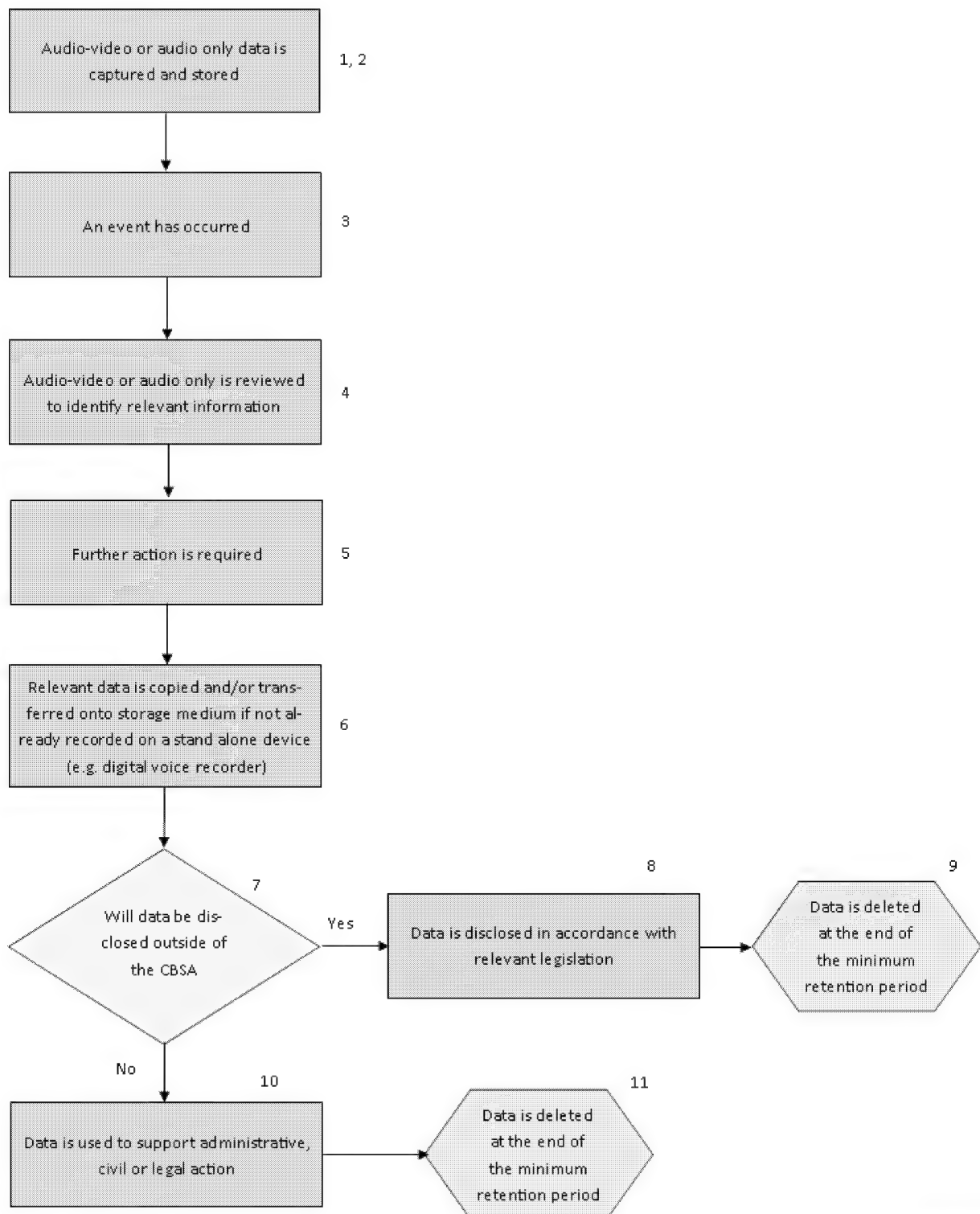
A grandfather clause has been written into the policy to ensure that any equipment that is already in use that is not capable of storing data for 30 days remains compliant with requirements. The minimum retention period for such equipment becomes the period for which the equipment is capable of storing data (e.g. if the equipment can only store data for 7 days, then the minimum retention period is 7 days). The grandfather clause expires when the equipment is replaced or upgraded.

All recordings and copies will be retained in accordance with the relevant CBSA security policy (Comptrollership Manual – Security Volume – Chapter 6: Storage of Sensitive Information and Assets).

5. If an event is identified or if an ATIP request or formal complaint is received, recordings must be reviewed to identify the applicable footage.
6. If the footage is reviewed to verify an event and a determination is made that no event occurred and no further action will be necessary in relation to the recording, the recording can be considered to be a transitory record.
7. The recording will not be disclosed outside the CBSA and will be deleted/disposed of upon the expiration of the minimum retention period of 30 days for transitory records.
8. If the footage is reviewed and it is determined that it contains an event, or if an ATIP request or formal complaint is received within 30 days of the creation of the recording, the footage will need to be copied to another storage location on the server, or to another storage medium such as a USB key or DVD (Information considered Protected C shall be encrypted) and will be retained for a minimum of two years in accordance with subsection 4(1) of the *Privacy Regulations*. All recordings and copies will be retained in accordance with the relevant CBSA security policy (Comptrollership Manual – Security Volume – Chapter 6: Storage of Sensitive Information and Assets).

9. The purpose for which the footage is being retained must be identified. If data will be disclosed outside the CBSA follow data flow #10. If data will not be disclosed outside the CBSA follow data flow #12.
10. If the recording is being retained in relation to an ATIP request, a formal complaint or if the event is related to a criminal offence that will be investigated by another law enforcement agency, the information may be disclosed outside of the CBSA. Any disclosure of video recordings will be made in accordance with all relevant legislation and policy, including the AV Policy.
11. The recording will be deleted/disposed of two years from the date that the last administrative action is taken with respect to it. Disposal of video recordings will be done in accordance with the policy found in the CBSA Comptrollership Manual – Security Volume, Chapter 8: Disposal of Sensitive Information and Assets.
12. If the event contained in the recording is related to an event concerning only the CBSA (i.e. CBSA employees only and should not be relevant to third parties), the information will not be disclosed outside of the Agency.
13. The recording will be deleted/disposed of two years from the date that the last administrative action is taken with respect to it. Disposal of video recordings will be done in accordance with the policy found in the CBSA Comptrollership Manual – Security Volume, Chapter 8: Disposal of Sensitive Information and Assets.

4.1a Audio and Audio-Video Data Flow Model - Diagram



Audio and Audio-Video Data Flow Explanatory Notes

1. Data is captured by means of cameras and or standalone audio capture devices that are plainly and clearly announced and/or are visible in their placement or use. If video is captured within an interview room, signs inform travellers and/or employees that an area is under surveillance.

Data is captured to provide evidence regarding offences relating to the acts and regulations that the CBSA governs at POEs

2. All audio and audio-video recordings are securely stored as per CBSA policies on the storage of protected information when they are not in use. (Refer to Appendix: Comptrollership Manual – Security Volume – Chapter 6: Storage of Sensitive Information and Assets).

Access to and control of any equipment used for recording purposes is limited to qualified operators who are authorized to do so by the manager responsible for the facility in which the equipment is located. Authorization is provided in writing and specifies the purposes for which access and or control is given.

3. Event – means any offences relating to the acts and regulations that the CBSA governs at POEs
4. Recordings must be reviewed to identify the applicable footage.
5. If the footage is reviewed to verify an event and a determination is made that no event occurred and no further action will be necessary in relation to the recording, the recording can be considered to be a transitory record.
6. The footage will need to be copied to another storage location on the server, or to another storage medium such as a USB key or DVD (Information considered Protected C shall be encrypted) and will be retained for a minimum of two years in accordance with subsection 4(1) of the *Privacy Regulations*. All recordings and copies will be retained in accordance with the relevant CBSA security policy (Comptrollership Manual – Security Volume – Chapter 6: Storage of Sensitive Information and Assets).
7. The purpose for which the footage is being retained must be identified.
8. If the recording is being retained in relation to a criminal offence that will be investigated by another law enforcement agency, the information may be disclosed outside of the CBSA. Any disclosure of video recordings will be made in accordance with all relevant legislation and policy, including the AV Policy.
9. The recording will be deleted/disposed of two years from the date that the last administrative action is taken with respect to it. Disposal of video recordings will be done in

accordance with the policy found in the CBSA Comptrollership Manual – Security Volume, Chapter 8: Disposal of Sensitive Information and Assets

10. If the event contained in the recording is related to an event concerning only the CBSA (i.e. CBSA employees only and should not be relevant to third parties), the information will not be disclosed outside of the Agency
11. The recording will be deleted/disposed of two years from the date that the last administrative action is taken with respect to it. Disposal of video recordings will be done in accordance with the policy found in the CBSA Comptrollership Manual – Security Volume, Chapter 8: Disposal of Sensitive Information and Assets

4.2 Example of a Data Flow Model - Table

Source of the personal information for the program or activity

From whom or from what organization is the personal information collected. In other words, identify who is providing the personal information that is being used, will be used or available for use for the program or activity. There may be more than one source, indicate all sources:

SOURCE	IDENTIFY THE SOURCE
The individual or a representative	Only the individual.
A federal government institution (identify from what PIB the information is obtained)	N/A
Non-federal institutions	
- Provincial Government	N/A
- Municipal Government	N/A
- Aboriginal Government/ Council	N/A
- Organization of a Foreign State	N/A
- International Organization	N/A
Private Sector	
- Located in Canada and Canadian Owned	In locations where CCTV equipment is not owned by the CBSA but installed in operational areas, airport or bridge authorities sometimes share video recordings with the CBSA. These locations are as follows: Windsor Tunnel Ambassador Bridge Bluewater Bridge Niagara-Whirlpool Bridge Fort Erie- Peace Bridge (Applicable to video only records obtained from the authority, and not applicable to audio and/or audio-video records obtained in interviews by the CBSA)

- Located in Canada and Foreign Owned	N/A
- Located abroad and Canadian Owned	N/A
- Located abroad and Foreign Owned	N/A

4.3 Internal Use and Disclosure

Where will that information circulate within the federal government institution? This must identify any related programs or activities and personal information banks as identified in the institution's Info Source chapter.

Program	Personal information bank
Ports of entry	CBSA PPU 1104
Investigations	CBSA PPU 026
Intelligence	N/A
Inland Enforcement	CBSA PPU 020, CBSA PPU 026,
Personnel Security and Professional Standards	CBSA PPE 813, CBSA PPU 039 (Not applicable to records obtained from interviews)

4.4 External Use and Disclosure

Where will that information circulate outside of the federal government institution? This includes any disclosure made to:

The individual or a representative	An individual or his/her representative may make an ATIP request with respect to his/her information.
A federal government institution	Records may be disclosed to other federal government institutions for the purpose of enforcing federal legislation.
Non-federal institutions and private sector	
- Provincial Government	Records may be disclosed to provincial law enforcement agencies for the purpose of enforcing federal legislation.
- Municipal Government	Records may be disclosed to municipal law enforcement agencies for the purpose of enforcing federal legislation.
- Aboriginal Government/ Council	
- Organization of a Foreign State	<i>Customs Act</i> 107(8) - This provision permits the CBSA to provide customs information to a foreign official of any of the entities listed in subsection 107(8) as long as it is in accordance with an international convention, agreement or other written arrangement between the Government of Canada or an institution of the Government of Canada and the government of the

	<p>foreign state, the organization, the community or the institution, solely for the purposes set out in that arrangement. The written collaborative arrangement could be an information sharing Memorandum of Understanding, a Customs Mutual Assistance Agreement, or other related instrument (See Section 5, 10.1.4 for list of countries)</p> <p>e.g. Canada has a Customs Mutual Assistance Agreement (CMAA) with the United Kingdom of Great Britain and Northern Ireland. The CMAA allows for the exchange of customs information, intelligence, and documents that assists each country in the prevention and investigation of customs offenses.</p>
- International Organization	
Private Sector	
- Located in Canada and Canadian Owned	<p>Recordings may be disclosed to private sector organizations such as Airport or Bridge Authorities when incidents involving employees of such Authorities or traffic accidents or other incidents for which the Authority may require footage. Such disclosures will only be made in accordance with the relevant legislative provisions and within the bounds of a clearly articulated Memorandum of Understanding. (Applicable to video only records, and not applicable to audio and/or audio-video records obtained in interviews)</p>
- Located in Canada and Foreign Owned	<p>Recordings may be disclosed to private sector organizations such as Airport or Bridge Authorities when incidents involving employees of such Authorities or traffic accidents or other incidents for which the Authority may require footage. Such disclosures will only be made in accordance with the relevant legislative provisions and within the bounds of a clearly articulated Memorandum of Understanding. (Applicable to video only records, and not applicable to audio and/or audio-video records obtained in interviews)</p>
- Located abroad and Canadian Owned	
- Located abroad and Foreign Owned	

4.5 Retention / Storage

Where will the information be stored or retained (identify all organizations that will store the information – this includes duplicates of the databases containing the personal information or any back-ups):

A federal government institution – within the CBSA	Recordings will be stored at the location where they are made. The recordings will be housed on secure servers
--	--

	<p>and in secure storage with access controls.</p> <p>In all cases where storage devices are used, they will be required to meet baseline physical security requirements based on the level of sensitivity of information gathered as per CBSA Security Volumes, depending on the recording medium.</p> <p>A copy of recordings disclosed to other federal government institutions, including federal law enforcement agencies, will be housed within those institutions or law enforcement agencies according to their requirements.</p>
A Federal Records Center	N/A
Non federal institutions and private sector	
1. Provincial Government	<p>A copy of recordings disclosed to provincial law enforcement agencies will be housed within those agencies according to their requirements.</p> <p><i>British Columbia Freedom of Information and Protection of Privacy Act:</i></p> <p>30.1 A public body must ensure that personal information in its custody or under its control is stored only in Canada and accessed only in Canada, unless one of the following applies:</p> <p>(a) if the individual the information is about has identified the information and has consented, in the prescribed manner, to it being stored in or accessed from, as applicable, another jurisdiction;</p> <p>(b) if it is stored in or accessed from another jurisdiction for the purpose of disclosure allowed under this Act;</p> <p>(c) if it was disclosed under section 33.1 (1) (i.1).</p> <p><i>Nova Scotia's Personal Information International Disclosure Protection Act:</i></p> <p>5 (1) A public body shall ensure that personal information in its custody or under its control and a service provider or associate of a service provider shall ensure that personal information in its custody or under its control is stored only in Canada and accessed only in Canada, unless</p> <p>(a) where the individual the information is about has identified the information and has consented, in the manner prescribed by the regulations, to it being stored in or accessed from, as the case may be, outside Canada;</p> <p>(b) where it is stored in or accessed from outside Canada for the purpose of disclosure allowed under this Act; or</p> <p>(c) the head of the public body has allowed storage or</p>

	<p>access outside Canada pursuant to subsection (2).</p> <p>(2) The head of a public body may allow storage or access outside Canada of personal information in its custody or under its control, subject to any restrictions or conditions the head considers advisable, if the head considers the storage or access is to meet the necessary requirements of the public body's operation.</p> <p>(3) Where the head of a public body makes a decision pursuant to subsection (2) in any year allowing storage or access outside Canada, the head shall, within ninety days after the end of that year, report to the Minister all such decisions made during that year, together with the reasons therefor.</p> <p>(4) In providing storage, access or disclosure of personal information outside Canada, a service provider shall only collect and use such personal information that is necessary to fulfill its obligation as a service provider, and shall at all times make reasonable security arrangements to protect any personal information that it collects or uses by or on behalf of a public body.</p> <p>Quebec's public sector privacy law, <i>An Act Respecting Access to Documents Held by Public Bodies and the Protection of Personal Information</i>:</p> <p>Not applicable as this applies to documents</p>
2. Municipal Government	A copy of recordings disclosed to municipal law enforcement agencies will be housed within those agencies according to their requirements.
- Aboriginal Government/ Council	N/A
- Organization of a Foreign State	N/A
- International Organization	N/A
Private Sector	
3. Located in Canada and Canadian Owned	A copy of recordings disclosed to any Airport or Bridge Authority will be housed within those Authorities according to their requirements, and as per the requirements of the MOU. (Applicable to video only records, and not applicable to audio and/or audio-video records obtained in interviews)
4. Located in Canada and Foreign Owned	A copy of recordings disclosed to any Airport or Bridge Authority will be housed within those Authorities according to their requirements, and as per the requirements of the MOU. (Applicable to video only records, and not applicable to audio and/or audio-video records obtained in interviews)
- Located abroad and Canadian Owned	N/A

- Located abroad and Foreign Owned	N/A
------------------------------------	-----

4.6 Other Possible Considerations

Identify the areas, groups and individuals who access and handle the personal information:

Identify the areas / groups / divisions who are allowed to access and handle the personal information collected for the program or activity. Also, identify where these areas or groups are located (i.e. national capital region, within a province, in a foreign country, or several locations if teleworking) as well as the location of the personal information to uncover any potential trans-border or inter-jurisdictional issues. When reasonable to do so, by virtue of the size of the organization or the number of individuals, identify individual positions rather than the work area or group.

Federal government Institution responsible for program or activity: <i>See Appendices for Inventory</i>		
Identify Groups or Areas / or Divisions	Positions who have access or use the personal information (where appropriate)	Geographical Location
Ports of entry	Chiefs, Supervisors and select Border Service Officers have access as part of their official duties at certain locations (Applicable to video only records, and not applicable to audio and/or audio-video records obtained in interviews).	The CBSA uses CCTV technology at 167 sites across Canada.
Investigations	Chiefs, Supervisors and Investigation Officers have access as part of their official duties at certain locations (Applicable to video only records, and audio and/or audio-video records obtained in interviews).	The CBSA uses CCTV technology at 167 sites across Canada. Handheld devices to record voice only can be used at all work locations.
Intelligence	Chiefs, Supervisors and Intelligence Officers have access as part of their official duties at certain locations (Applicable to video only records, and audio and/or audio-video records obtained in interviews).	The CBSA uses CCTV technology at 167 sites across Canada. Handheld devices to record voice only can be used at all work locations.
Inland Enforcement	Chiefs, Supervisors and Inland Enforcement Officers have access as part of their official duties at certain locations (Applicable to video only records, and audio and/or audio-video records obtained in interviews).	The CBSA uses CCTV technology at 167 sites across Canada. Handheld devices to record voice only can be used at all work locations.
Personnel Security and Professional Standards	Various positions (Applicable to video only records on a need to know basis, and not applicable to audio and/or audio-video records obtained in interviews)	The CBSA uses CCTV technology at 167 sites across Canada
Other federal government Institution responsible for program or activity: (one table per institution):		
N/A		
Non Federal Institution or Private Sector: 'name': (one table per institution)		
N/A		

Overt Use of Video Monitoring and Recording Technology

PIA

SECTION 5 - PRIVACY COMPLIANCE ANALYSIS

Legal Authority For Collection Of Personal Information

Has a legal authority been identified for the collection of personal information for this program or activity?

Statutory reference: Section 4 of *Privacy Act* (Section 4 has been interpreted to mean that a legal authority must be established for a collection of personal information, but section 4 does not provide legal authority for such a collection).

Policy reference: Section 6.2.6 of *Directive on Privacy Practices*

Yes

- 1.1 ☒ Please specify the legal authority and briefly explain its connection to the program or activity or how it permits the collection of the personal information:

Canada Border Services Agency Act, paragraph 5(1)(a)

If legal authority is unclear consult your Legal Service to determine authority for the program or activity.

The CBSA's use of electronic recordings is directly related to paragraph 5(1)a of the CBSA Act and does not raise high risks of violating section 8 of the *Charter* nor section 4 of the *Privacy Act* as long as the information captured is used within set limitations.

- 1.2 ☒ AND, ensure that the legal authority to collect the personal information is cited in the relevant PIB and in "Section I – Overview and PIA Initiation" of the PIA.

→ Continue to Question 2

No

- 1.3 ☐ If there is no legal authority for the collection of personal information, it cannot be collected. Please consult your institution's legal advisors to determine if there is authority to proceed with the program or activity.

Necessity To Collect Personal Information

Is each element and sub-element of personal information collected or to be collected necessary to administer the program or activity?

Statutory reference: Section 4 of *Privacy Act*

Policy reference: Sections 6.1.1, 6.1.3, 6.1.4, 6.2.7 and 6.2.8 of *Directive on Privacy Practices*

YES

- 2.1 ☒ Ensure that all personal information necessary to administer the program or activity is listed in the relevant PIB.
- 2.2 ☒ AND, implement controls and procedures to ensure the institution does not collect more personal information than is necessary for the identified program or activity and that a continuing need exists for that information or its collection.

→ Continue to Question 3

NO

- 2.3 ☐ Review the proposed elements and sub-elements of personal information outlined in "Section 3 – Analysis of Personal Information Elements" to identify those that are "necessary" and not merely

useful. Document any changes.

Authority For the Collection, Use or Disclosure Of the Social Insurance Number

Is the collection of the Social Insurance Number (SIN) necessary to administer the program or activity?

Statutory reference: Section 4 of *Privacy Act*

Policy reference: Section 6.2.13 of *Policy on Privacy Protection* and sections 6.1.1 and 6.2 to 6.4 of *Directive on Social Insurance Number*

Also see "Guidance for Preparing Information-Sharing agreements Involving Personal Information" and "Taking Privacy into Account Before making Contracting Decisions"

YES

- 3.1 ☐ Collection of the SIN must be in compliance with the *Directive on Social Insurance Number* (please check all appropriate boxes below):
- 3.2 ☐ State legal authority for collecting the SIN:

OR, in the absence of a legal authority to collect the SIN:

- 3.3 ☐ Establish explicit authority through legislative amendment(s).
- 3.4 ☐ Establish legal authority as outlined in the *Directive on Social Insurance Number*.

AND, if disclosure of the SIN by the institution is to occur on a routine or systematic basis

- 3.4.1 ☐ to another federal institution that is authorized to collect it, or to another level of government, establish an agreement or arrangement that includes specific provisions to limit the use of the SIN.
- 3.4.2 ☐ to a contractor or other external service provider, establish a contract that includes specific provisions to limit the use of the SIN.
- 3.5 ☐ AND, ensure that the relevant PIB for the program or activity states the authority under which the SIN is collected and the purpose for which it is used.

→ Continue to Question 4

NO

- 3.6 ☒ The SIN is not necessary and it will not be collected, used or disclosed to administer the program or activity.

→ Continue to Question 4

Direct Collection - Notification and Consent (as appropriate)

Is personal information collected directly from the individual to whom it relates?

Statutory reference: Sections 4 and 5 of *Privacy Act*

Policy reference: Sections 6.1.1, 6.2.6 and 6.2.9 to 6.2.13 of *Directive on Privacy Practices* and section 6.1.2 and 6.4.1 of *Directive on Social Insurance Number*

YES

- 4.1 ☒ A "Privacy Notice" (adapted for either verbal or written communications) must be provided to the individual at the time of collection and it must notify the individual of any of the following elements

that apply (please check all appropriate boxes):

- ☒ a) The purpose and authority for the collection
- ☒ b) Any uses or disclosures that are consistent with the original purpose.
- ☐ c) Any uses or disclosures that are not related to the original purpose
- ☐ d) Any legal or administrative consequences for refusing to provide the personal information
- ☒ e) That the "individual to whom the information relates" has rights of access to, correction of and protection of personal information under the *Privacy Act*. (Applicable to video only records, and not applicable to audio and/or audio-video records obtained in interviews)
- ☐ f) A reference to the PIB for the program or activity
- ☐ g) Why the SIN is collected, how it will be used and the consequence of not providing it.

AND, add a **"Consent Statement"** to the **"Privacy Notice"** as appropriate, if the personal information is to be used or disclosed for a purpose other than the original purpose or a consistent use, or, to authorize indirect collection of personal information.

- 4.2 ☐ The **"Consent Statement"** must include, as applicable, the following elements (please check all appropriate boxes):
- ☐ a) The purpose of the consent and the specific personal information involved.
 - ☐ b) In the case of indirect collections, the sources that will be asked to provide the information.
 - ☐ c) Uses and disclosures that are not consistent with the original purpose of the collection and for which consent is being sought.
 - ☐ d) Any consequences that may result from withholding consent.
 - ☐ e) Any alternatives to providing consent
- 4.3 ☐ AND, implement controls and procedures to ensure that the institution keeps a record documenting whether or not an individual provided consent when it was sought, including a record documenting any withdrawal of consent when applicable.
- Continue to Question 5

NO

- 4.4 ☐ The personal information necessary for the program or activity is not collected directly from the individual. It is collected indirectly, for example, from another program within the institution, or from another institution, government or third party.
- Continue to Question 5

Indirect Collection - Consent or Authority Under Sec. 10 of Privacy Regulations

Is personal information collected indirectly from another source with the informed consent of the individual to whom it relates, or from a person authorized to act on behalf of the individual pursuant to section 10 of the Privacy Regulations?

Statutory reference: Sections 4 and 5 of *Privacy Act* and section 10 of *Privacy Regulations*

Policy reference: Sections 6.1.1, 6.2.6 and 6.2.9 to 6.2.13 of *Directive on Privacy Practices* and sections 6.1.2 and 6.4.1 of the *Directive on Social Insurance Number*

YES

- 5.1 ☐ The notice and consent requirements stated at Question 4 apply. Please review the required elements listed under "YES" at Question 4 and check the corresponding boxes below to indicate the elements that need to be included in the "Privacy Notice" or the "Consent Statement" (check all that apply):

Privacy Notice	a) <input type="checkbox"/>	b) <input type="checkbox"/>	c) <input type="checkbox"/>	d) <input type="checkbox"/>	e) <input type="checkbox"/>	f) <input type="checkbox"/>	g) <input type="checkbox"/>
Consent Statement	a) <input type="checkbox"/>	b) <input type="checkbox"/>	c) <input type="checkbox"/>	d) <input type="checkbox"/>	e) <input type="checkbox"/>		

- 5.2 ☐ AND, implement controls and procedures to ensure the institution keeps a record documenting whether or not an individual provided consent when it was sought, including a record documenting any withdrawal of consent when applicable.
- 5.3 ☐ AND, if information is being collected from persons authorized to act on behalf of minors, incompetents or individuals who have been deceased for less than 20 years, implement appropriate mechanisms to ensure that such persons are authorized to act on behalf of individuals who do not have the capacity to provide consent.

→ Continue to Question 6

NO

- 5.4 ☒ → Continue to Question 6

Indirect Collection - Without Notification and Consent

Is personal information collected from another source without notice to or consent from the individual to whom the information relates?

Statutory reference: Sections 4, 5, 7 and 8 of *Privacy Act* and section 10 of *Privacy Regulations*

Policy reference: Sections 6.2.6 and 6.2.9 to 6.2.13 of *Directive on Privacy Practices*, section 6.2.15 of the *Policy on Privacy Protection* and sections 6.3.2 and 6.3.3 of *Directive on Privacy Impact Assessment*

YES

- 6.1 ☐ Where information is collected indirectly under any of the following circumstances without notice to, or consent from, the individual to whom it relates, please check the applicable boxes and explain as requested:
- ☐ a) The collection is a result of a disclosure to the institution under subsection 8(2) of the *Privacy Act*. State the applicable paragraph(s) of subsection 8(2) and provide a brief explanation for each:
-
- ☐ b) Direct notification of the individual might result in the collection of inaccurate information, or might defeat the purpose or prejudice the use for which the information is collected. Briefly explain why notice is not provided
-
- ☐ c) The information involved in the program or activity is to be used solely for a non-administrative purpose in which no decisions are made about the individuals to whom the information relates.

- 6.2 ☐ AND, if any of the circumstances in a) b) or c) is applicable, ensure that it is reflected in the relevant PIB.
- 6.3 ☐ AND, if the information is to be used solely for a non-administrative purpose (box c above has been checked), ensure that the requirements under sections 6.3.2 and 6.3.3 of the *Directive on Privacy Impact Assessment* have been met, and that the decision of the official responsible for section 10 of the *Privacy Act* to proceed with a PIA for the program or activity has been adequately documented in the description of the program or activity in "Section I - Overview and PIA Initiation" of the PIA.
- 6.4 ☐ OR, if none of the circumstances in a) b) or c) is applicable, then the personal information must be collected directly from the individual, or indirectly with the consent of the individual. Please review the responses to Questions 4 and 5 and ensure that the "Privacy Notice" or the "Consent Statement" includes all of the required elements listed under "YES" at Question 4.
- Continue to Question 7

NO

- 6.5 ☒ All personal information is collected directly from the individual to whom it relates, or from another source with notice to, or consent from, the individual or a person authorized to act on behalf of the individual (see Questions 4 and 5 above).
- Continue to Question 7

Retention and Disposal of Personal Information

Has Library and Archives Canada approved a records retention and disposal schedule that applies to the personal information?

Statutory reference: Section 12 of *Library and Archives Canada Act*, sections 6, 10 and 11 of *Privacy Act* and section 4 of *Privacy Regulations*

Policy reference: Sections 6.1.3, 6.2.11 to 6.2.13 and 6.2.23 of *Directive on Privacy Practices*

YES

- 7.1 ☒ Please identify the Record Disposition Authority (RDA) and describe the retention and disposal schedule:

For any record considered to be a transitory record, the RDA is MIDA 90/000: transitory records will be retained for 30 days and will be destroyed within 15 days of the expiration of that retention period.

Recordings of any video monitoring activity must be retained for no less than thirty (30) days following the date of their creation. Recordings that are used to obtain or provide information or to investigate an allegation or complaint, or used as evidence in respect of an identifiable individual shall be kept for the longer of two (2) years following the date of their creation, or following the date of their last use in an administrative action as information or as evidence in respect of that person.

A RDA has been requested from Library and Archives Canada for all records which are not considered to be transitory. The request has not yet been approved; however it is the intention of the CBSA to retain these records in accordance with paragraph 4(1)(a) of the *Privacy Regulations*, for a minimum of two years from the date of their creation.

- 7.2 ☒ AND, implement controls and procedures to ensure that personal information used to make a decision that directly affects an individual will be retained for a minimum of two years after the last administrative action or, where a request for access to the information has been received, until such

time as the individual has had the opportunity to exercise all his/her rights under the Act)

7.3 ☐ AND, if the institution intends to dispose of personal information that has been used for an administrative purpose prior to the expiration of the two-year minimum retention standard established by the *Privacy Regulations*, it must obtain the consent of the individual to whom the information relates before doing so.

7.4 ☒ AND, the institution must cite the RDA number, the retention period and the disposition standards for the personal information in the relevant PIB.

→ Continue to Question 8

NO

7.5 ☒ Provide a Records Disposition Submission to Library and Archives Canada describing the records containing the personal information for which the institution requires a RDA.

The CBSA has requested a RDA for all audio-video records that are not considered to be transitory.

7.6 ☒ AND, obtain a RDA from Library and Archives Canada to allow the institution, under certain conditions, to dispose of records that no longer have operational utility for the program or activity.

7.7 ☒ AND, ensure that all the other applicable requirements listed under "YES" at Question 7 are met.

→ Continue to Question 8

Accuracy Of Personal Information

Will measures be adopted to ensure that personal information used by the institution for an administrative purpose is as accurate, up-to-date and complete as possible?

Statutory reference: Sections 6, 10 and 11 of *Privacy Act* and sections 10 and 11 of *Privacy Regulations*

Policy reference: Sections 6.1.1 and 6.2.9 to 6.2.16 of *Directive on Privacy Practices*

YES

8.1 ☐ Please check any of the following measures that will be adopted to ensure accuracy of the personal information and provide details as requested:

8.1.1 ☒ Personal information will be collected directly from the individual to whom it relates or it will be validated with the individual or a person authorized to act on behalf of the individual.

8.1.2 ☐ A data-matching process will be used to verify the accuracy of personal information against a "reliable source" (within or outside the institution) where this is authorized, or where consent was obtained. Please briefly describe the data-matching process and the source(s) that will be used to ensure accuracy of the information:

8.1.3 ☐ In cases where direct collection or consent is not feasible, the institution will obtain information from trusted sources (public or private) and verify accuracy against existing personal information before use. Please identify the sources and procedures to be used to check the accuracy of the information:

8.1.4 ☐ Technological methods will be used to identify errors and discrepancies. Please briefly describe these technological methods:

8.1.5 ☐ Other – please specify:

8.2 ☐ AND, if measures are adopted other than "*direct collection or validation with the individual or with a person authorized to act on behalf of the individual*", the institution must implement appropriate controls and procedures to ensure that:

- a) the technique(s) and the specific source(s) used to validate or update the personal information are documented;
- b) individuals are given the opportunity, whenever possible, to request correction of any inaccurate personal information before the information is used in a decision-making process that affects them;
- c) personal information can only be modified or corrected by those within the institution who have the authority to do so; and
- d) when personal information is corrected or annotated, other authorized holders of the information are notified about the correction or annotation and that all copies of the information in the possession of the institution are corrected / annotated.

8.3 ☐ AND, if appropriate, ensure that the "**Privacy Notice**" or "**Consent Statement**" and the relevant PIB are amended to identify the data-matching activity including the source(s).

→ Continue to Question 9

NO

8.4 ☐ Please explain why such measures will not be adopted:

→ Continue to next Question 9

Use Of Personal Information

Will the personal information collected for the program or activity be used solely for the original purpose for which it was obtained or compiled, a use consistent with that purpose, or a purpose for which the information was disclosed to the institution pursuant to subsection 8(2) of the Privacy Act?

Statutory reference: Sections 5 and 7 to 11 of *Privacy Act*

Policy reference: Sections 6.1.1, 6.1.9, 6.2.9 to 6.2.13 and 6.2.17 of *Directive on Privacy Practices*, section 6.2.15 of *Policy on Privacy Protection* and Section IV of Appendix C of *Directive on Privacy Impact Assessment*

YES

9.1 ☒ Implement controls and procedures to ensure that access to the personal information for such

purposes will be limited to authorized individuals who need to know the information to perform their official duties

9.2 ☒ AND, ensure that the "Data Flow Diagram" or "Data Flow Tables" completed for "Section IV – Flow of Personal Information" of the PIA identify the areas, groups and individuals (e.g., the positions) within the institution who have a need-to-know to access to or handle the personal information, including their geographical location and where the personal information will be stored or retained.

9.3 ☒ AND, if the purposes for which the personal information is used includes any use(s) of the information for a non-administrative purpose, (such as research, statistical, audit and evaluation purposes) the institution will adhere to the requirements and principles in its "**Privacy Protocol For Non-Administrative Purposes**", in accordance with section 6.2.15 of the *Policy on Privacy Protection*, to address any impact that such non-administrative uses may have on privacy.

→ Continue to Question 10

NO

9.4 ☐ Identify below any other uses of the personal information, in other words, any routine uses that are not directly related to the purpose of the collection, or, which are not consistent with that purpose or for which the information was disclosed to the institution pursuant to subsection 8(2) of the *Privacy Act*:

9.5 ☐ AND, ensure that these other uses are reflected in the relevant PIB

9.6 ☐ AND, include a description of these other uses in the "**Privacy Notice**" or "**Consent Statement**", as appropriate,

☐ AND, ensure the all the other applicable requirements listed under "**YES**" at Question 9 are met.

→ Continue to Question 10

Disclosures Directly Related to the Administration of the Program or Activity

Will personal information be disclosed for purposes directly related to the administration of the program or activity?

Statutory reference: Sections 5 and 8 to 11 of *Privacy Act*.

Policy reference: Sections 6.2.10, 6.2.11 and 6.2.13 of *Policy on Privacy Protection*, sections 6.2.1 to 6.2.3 of *Directive on Social Insurance Number*, sections 6.1.9, 6.2.9 to 6.2.13 and 6.2.15 to 6.2.20 of *Directive on Privacy Practices* and section IV of Appendix "C" of *Directive on Privacy Impact Assessment*)

Also see "Guidance for Preparing Information-Sharing agreements Involving Personal Information" and "Taking Privacy into Account Before making Contracting Decisions"

YES

10.1 ☒ Please check all applicable boxes below and, for each disclosure, identify the name of the organization or third party to which personal information will be disclosed. If it is disclosed within the institution, please identify the branch and the program or activity.

10.1.1 ☒ Within the institution for another program or activity – specify

Criminal Investigations, Security and Professional Standards, Intelligence, Inland Enforcement

10.1.2 ☒ Other federal government institutions – specify

Royal Canadian Mounted Police, Canadian Security Intelligence Service

10.1.3 ☒ Provincial, territorial or municipal governments institutions – specify

Provincial, municipal and local police agencies, such as the Ontario Provincial Police, the Sûreté du Québec, and Halifax Regional Police

10.1.4 ☒ Foreign government institutions and entities thereof – specify

Written Collaborative Arrangements exist between the CBSA and the following countries:

10.1.5 ☐ International organizations – specify

10.1.6 ☒ The private sector (e.g., contractor or other external service provider) – specify

Airport and Bridge Authorities, such as the Greater Toronto Airport Authority (Applicable to video only records, and not applicable to audio and/or audio-video records obtained in interviews)

10.1.7 ☐ Other – specify

10.2 ☒ AND, ensure that:

- a) any such disclosure is made in compliance with section 8 of the *Privacy Act*, which allows disclosures of personal information with consent of the individual to whom the information relates (subsection 8(1)) or without consent in certain and limited circumstances pursuant to subsection 8(2) of the Act;
- b) only personal information elements that are necessary for the intended purpose are disclosed;
- c) the organization or third party receiving the personal information is authorized to do so;
- d) administrative, physical and technical safeguards appropriate to the sensitivity of the information will be applied to protect the information during and after its transmission (see Question 15);
- e) the organization or third party to which the personal information will be disclosed for the administration of the program or activity are identified in the “Consistent Use” section in the relevant PIB in *Info Source*, including the specific purpose of the disclosure;
- f) the “**Privacy Notice**” or “**Consent Statement**” describes any disclosures of information; and,
- g) the “Data Flow Diagram” or “Data Flow Tables” completed in “Section IV – Flow of Personal Information” of the PIA include details on the disclosed personal information:

10.3 ☒ AND, any disclosure of personal information to another federal institution or outside the Government of Canada is governed by a formal agreement or arrangement (e.g., a Memorandum of Understanding, an accord, a contractual arrangement, etc.) to ensure that appropriate privacy protection clauses are included, and, where applicable, include provisions for inter-jurisdictional or transborder flows of personal information. Such clauses must cover the following topics:

- a) Control over personal information, where appropriate.
- b) Limitations on the collection, retention, use and disclosure of personal information.
- c) Measures (administrative, technical and physical) to protect the integrity and confidentiality of personal information.
- d) Measures governing the disposition of the personal information, where relevant
- e) Measures to ensure or verify that the personal information is only used for the purposes related to the agreement, arrangement or contract.
- f) Obligations are to be extended to other parties such as subcontractors.

→ Continue to Question 11

NO

10.4 ☐ There is no disclosure of personal information within or outside the institution for purposes that are

directly related to the administration of the program or activity.

→ Continue to Question 11

Accounting For New Uses or Disclosures Not Reported in Info Source

Will controls and procedures be implemented to account for any new use or disclosure of the personal information that is not included in the relevant PIB published in Info Source?

Statutory reference: Sections 7 to 11 of *Privacy Act* and section 4 of *Privacy Regulations*

Policy reference: Sections 6.1.9 and 6.2.2 of *Directive on Privacy Practices*

YES

11.1 ☒ Appropriate controls and procedures have been or will be implemented to ensure that:

- a) the head of the institution or the appropriate delegate is notified about any new use or disclosure of personal information that is not reflected in the PIB description published in *Info Source*;
- b) the consent of the individual to whom the information relates is obtained in writing, as appropriate, prior to any new use of the information for an administrative purpose that is not reflected in the relevant PIB published in *Info Source*, unless the new use is considered to be consistent with the purpose for which the personal information was obtained or compiled and the Privacy Commissioner is notified forthwith regarding the new consistent use;
- c) except as permitted under subsection 8(2) of the *Privacy Act*, any disclosure of personal information for a purpose that is not reflected in the relevant PIB published in *Info Source* will only be made with the consent of the individual to whom the information relates;
- d) a record is kept for any new use or disclosure of personal information not described in the relevant PIB published in *Info Source*, and that this record is stored with the personal information to which it relates and retained for a minimum period of two years following such a use or disclosure
- e) if the information is disclosed to a federal investigative body under paragraph 8(2)(e) of the *Privacy Act*, the record of disclosure will be kept in a separate PIB for a period of two years where it will be available to the Privacy Commissioner for review upon request;
- f) the Privacy Commissioner is notified forthwith, as required under subsection 9(4) of the Act, of any new use or disclosure that is consistent with the purpose for which the information was obtained or compiled, but which is not reflected in the relevant PIB published in *Info Source*;
- g) the relevant PIB is amended in time for the next edition of *Info Source* to include any new use(s) or disclosure(s) that are consistent with the purpose for which the information was obtained or compiled, as well as any routine use(s) or disclosure(s) that do not fall within the categories of purpose of collection or consistent use; and
- h) the Privacy Commissioner is notified prior to or forthwith, as required under subsection 8(5) of the Act, about any disclosures made or to be made in the public interest or in the interest of the individual to whom the information relates.
- i) Other, specify

→ Continue to Question 12

NO

- 11.2 ☐ Please explain why such controls and procedures will not be implemented (provide adequate justification):

→ Continue to Question 12

Safeguards - Statement Of Sensitivity

Has a Statement of Sensitivity (SoS) or similar analysis been completed to assess the degree of sensitivity of the personal information to be collected and retained for the program or activity?

Statutory reference: Sections 7 and 8 of *Privacy Act*.

Policy reference: Appendix C of *Directive on Privacy Impact Assessment* and sections 6.2.17 to 6.2.21 of *Directive on Privacy Practices*, *Policy on Government Security*, *Operational Security Standard: Management of Information Technology Security (MITS)*

YES

- 12.1 ☒ The information contained in the SoS or similar analysis has been taken into account when assessing the level of risks to privacy in "Section 2 - Risk Area Identification and Categorization" of the PIA.

→ Continue to Question 13

NO

- 12.2 ☐ Please explain why a SoS or similar analysis was not considered necessary to assess the sensitivity of the information.

→ Continue to Question 13

Safeguards - Threat and Risk Assessment

Has a Threat and Risk Assessment (TRA) or a similar security assessment been completed for the program or activity?

Statutory reference: Sections 7 and 8 of *Privacy Act*.

Policy reference: Appendix C of *Directive on Privacy Impact Assessment* and sections 6.2.17 to 6.2.21 of *Directive on Privacy Practices*, *Policy on Government Security*, *Operational Security Standard: Management of Information Technology Security (MITS)*

YES

- 13.1 ☒ Reference the title of the TRA or other security assessment in "Section VII – Supplementary Documents List" and provide a brief synopsis of the assessment in the space below:

TRAs have been completed for 8 sites, representing highway (land and bridge), air, rail, marine, inland and commercial operations.

The TRAs have identified eleven significant residual risks as stated in the attached summary and noted that the residual risk level for each site is: **High**

The TRAs have identified 54 recommendations to mitigate the assessed risks to a lower level.

Once the 54 recommendations are fully implemented the overall projected residual risk level for this assessment is: **Low**

13.2 ☐ AND, obtain assurances from the officials responsible for the program or activity that the measures recommended in the assessment have been implemented to ensure the confidentiality, availability and integrity of the personal information.

13.3 ☐ AND, ensure that any residual risks to personal information are known and accepted by the executive or senior official responsible for the program or activity and the Head or delegated authority for the *Privacy Act*.

→ Continue to Question 14

NO

13.4 ☐ If a TRA or similar security assessment is underway, simply reference that fact in the space below and indicate when it is likely to be completed. If there is no intent to complete one, please explain.

→ Continue to Question 14

Safeguards - Administrative, Physical and Technical

Please identify below any administrative, physical and technical safeguards in place, or to be implemented, for this program or activity to ensure the confidentiality, availability and integrity of the personal information.

Statutory reference: Sections 7 and 8 of *Privacy Act*

Policy reference: Appendix C of *Directive on Privacy Impact Assessment* and sections 6.2.17 to 6.2.21 of *Directive on Privacy Practices*, *Policy on Government Security*, *Operational Security Standard: Management of Information Technology Security (MITS)*

Please check all that apply, including safeguards identified by the TRA or similar security assessment.

14.1 Administrative safeguards

- ☒ Internal security and privacy policies and procedures
- ☒ Staff training on privacy and the protection of personal information
- ☒ Screening and security checks of employees
- ☒ Appropriate security levels for employees who will have access to personal information
- ☒ Contingency plans and documented procedures in place to identify and respond to security and privacy breaches
- ☐ Regular monitoring of users' security practices
- ☒ Methods to ensure that only authorized personnel who need to know have access to personal information
- ☐ Other – please describe

14.2 Physical safeguards

- ☒ Restricted access areas
- ☐ Security guards
- ☒ Identification badges are worn by staff at all times
- ☒ After hours alarms and monitoring systems
- ☒ Locked filing cabinets
- ☐ Combination locks
- ☒ Safes
- ☐ Cipher locks
- ☒ Key cards
- ☒ Video surveillance (closed-circuit television)
- ☒ Secured server locations
- ☐ Backups secured off-site
- ☐ Other – please describe

14.3 Technical safeguards

- ☒ Role-based user authorization and authentication
- ☐ Biometrics
- ☐ Passwords (minimum of 6 characters long, include alpha and numeric characters)
- ☐ Passwords are changed by users every 90 days and recently used passwords cannot be re-used)
- ☐ Password protected screensavers
- ☐ Session-time out security (automatically locks an account after a session has been idle for a specified amount of time)
- ☐ Firewalls
- ☐ Intrusion Detection System (IDS)
- ☐ Virtual Private Network (VPN)
- ☐ Encryption of sensitive information
- ☐ Government of Canada Public Key Infrastructure Certificates (PKI)
- ☐ External Certificate Authority (CA)
- ☐ Audit trails
- ☐ Other – please describe

→ Continue to Question 15

Technology and Privacy - Tracking Technologies

Will the information system(s) used to deliver the program or activity employ cookies or other tracking technologies to collect personal information about users and their transactions?

Statutory reference: Sections 4 to 10 of the *Privacy Act* and section 4 of *Privacy Regulations*

Policy reference: Subsections 6.1.1, 6.1.3, 6.1.9, 6.2.9 to 6.2.13, 6.2.17 and 6.2.23 of *Directive on Privacy Practices*

YES

- 15.1 ☐ The specific tracking technologies to be used is adequately described under Part F: Technology and Privacy of "Section II – Risk Area Identification and Categorization" of the PIA;
- 15.2 ☐ AND, the collection of any personal information using such technologies is reflected in the relevant PIB and in "Section III – Analysis of Personal Information Elements" of the PIA;
- 15.3 ☐ AND, the use of such technologies to collect information about users and their transactions is adequately reflected in the "Privacy Notice";
- 15.4 ☐ AND, those responsible for implementing and using tracking technologies to collect personal information or who may have access to personal information collected through these methods are made aware of privacy and security policy requirements;
- 15.5 ☐ AND, where personal information collected through such tracking technologies is used to make a decision that directly affects the individual to whom the information relates, it will be retained for a minimum of two years after the last administrative action as required under the *Privacy Regulations*.
 → Continue to Question 16

NO

- 15.6 ☒ Tracking technologies are not used to collect personal information about users.
 → Continue to Question 16

Technology and Privacy - Surveillance or Monitoring

Will the new or modified program or activity result in new or increased surveillance or monitoring of a targeted population?

Statutory reference: Sections 4 to 10 of *Privacy Act*, section 4 of *Privacy Regulations* and section 8 of the *Charter of Rights and Freedoms*

Policy reference: Subsections 6.1.1, 6.1.9, 6.2.9 to 6.2.13 and 6.2.17 of *Directive on Privacy Practices*

YES

- 16.1 ☒ Consult with your legal advisors to determine whether or not such surveillance or monitoring activities raise any issues relating to the *Charter of Rights and Freedoms*, the *Privacy Act* or other applicable acts.
- 16.2 ☒ And, ensure the surveillance or monitoring method(s) to be used, the characteristic(s) of the targeted population and the scope of the surveillance or monitoring are adequately described under Technology and Privacy of "Section II – Risk Area Identification and Categorization" of the PIA.
- 16.3 ☒ AND, any personal information collected or created as a result of such surveillance or monitoring is described in the relevant PIB and in *Section III – Analysis of Personal Information Elements* of the PIA.
- 16.4 ☒ AND, the collection or use of personal information through surveillance or monitoring is adequately

reflected in the "**Privacy Notice**", unless such notification might result in the collection of inaccurate information or defeat the purpose or prejudice the use for which the personal information is collected.

☐ If notice about surveillance or monitoring will not be provided, please explain why:

16.5 ☒ AND, those responsible for implementing and using such surveillance or monitoring method(s) or who may have access to personal information collected or created through these methods are made aware of privacy and security policy requirements.

→ Continue to Question 17

NO

16.6 ☐ The new or modified program or activity will not result in surveillance or monitoring.

→ Continue to Question 17

Considerations Related to Compliance, Regulatory Investigation, Enforcement

Does the program or activity involve compliance/regulatory investigation or law enforcement, surveillance or intelligence gathering that targets specific individuals against whom penalties, criminal charges or sanctions may be applicable?

Statutory reference: Sections 4 to 10 of *Privacy Act*, section 4 of *Privacy Regulations* and section 8 of the *Charter of Rights and Freedoms*

Policy reference: Subsections 6.1.1, 6.1.9, 6.2.9 to 6.2.13 and 6.2.17 of *Directive on Privacy Practices*

YES

17.1 ☒ Consult with your legal advisors to determine whether or not the compliance/regulatory investigation or law enforcement activities raise any issues relating to the *Charter of Rights and Freedoms*, the *Privacy Act* or other applicable acts.

17.2 ☒ AND, identify the legislative authority and the specific regulatory or law enforcement purpose involved:

The activity is undertaken in accordance with *Canada Border Services Agency Act*, paragraph 5(1)(a)

17.3 ☐ AND, if the legislative authority differs from the legal authority for the program or activity, ensure it is adequately reflected in the response to Question 1 of "*Section V – Privacy Compliance Analysis*" and in "*Section I – Overview and PIA Initiation*" of the PIA.

17.4 ☒ AND, any personal information collected or created as a result of such regulatory or criminal enforcement, surveillance or intelligence gathering program or activity is described in the relevant PIB and in "*Section III – Analysis of Personal Information Elements*" of the PIA.

17.5 ☒ AND, the collection or use of personal information through these compliance / regulatory investigation or enforcement activities is adequately reflected in the "**Privacy Notice**", unless such notification might result in the collection of inaccurate information or defeat the purpose, or prejudice the use, for which the personal information is collected.

☐ If notice about the compliance/regulatory investigation or law enforcement activities will not be provided, please explain why:

NO

17.6 ☐ The program or activity does not involve the conduct of regulatory or criminal enforcement, surveillance or intelligence gathering.

Note: The table below can be used to keep an account of actions completed and to track outstanding actions required to achieve privacy compliance:

Privacy Compliance Analysis question #	Action required to support legal and policy compliance (cross reference to relevant question of <i>Section 5 – Privacy Compliance Analysis</i>)	Done	To be done
1	Legal authority for the program has been established and is reflected in the relevant PIB.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2	a) The categories and elements of personal information to be collected for the new program have been carefully assessed based, for example, on the institution's experience gained with the administration of a similar program. The personal data collected will be limited to only that which is required.) b) These categories and elements of personal information have been described in the relevant PIB for the program. c) Controls and procedures will be implemented to ensure that the institution does not collect more personal information than necessary for the program and that a continuing need exists for that information and its collection.	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
4 and 5	a) All of the requisite "Privacy Notices" and "Consent Statements" that meet the requirements of sections 6.2.9 to 6.2.12 of the <i>Directive on Privacy Practices</i> have been drafted. (Texts of the notices and consent statements may be included here.) ***To be posted on the CBSA web site*** b) Controls and procedures have been implemented to keep records of individual consents, and to ensure that persons acting on behalf of individuals who do not have the capacity to provide consent have the authority to do so under section 10 of the <i>Privacy Regulations</i> .	<input type="checkbox"/> <input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> <input type="checkbox"/>
7	a) A Records Disposal Authority (RDA) has been approved by Library and Archives Canada to authorize the disposal of the records containing personal information for the program. b) Controls and procedures have been implemented within the program and the ATIP Office to ensure that information that has been used for an administrative purpose will be kept for the	<input type="checkbox"/> <input checked="" type="checkbox"/>	<input checked="" type="checkbox"/> <input type="checkbox"/>

Overt Use of Video Monitoring and Recording Technology

PIA

	minimum retention period established by the Privacy Regulations.		
	c) Reference to the RDA, the retention period and the disposition standards for the program have been cited in the relevant PIB.	<input type="checkbox"/>	<input checked="" type="checkbox"/>
8	Controls and procedures are in the process of being implemented to ensure that the personal information associated with the program is as accurate, complete and up-to-date as necessary.	<input checked="" type="checkbox"/>	<input type="checkbox"/>

SECTION 6 - Summary of Analysis and Recommendations

****Please see PIA Action Plan****

SECTION 7 - SUPPLEMENTARY DOCUMENTS LIST

Additional documents used or related to the PIA may include:

- *CBSA Policy on the Overt Use of Audio-Video Monitoring and Recording Technology*
- *CBSA Directives on the Overt Use of Audio Video Monitoring and Recording Technology*
- CBSA Comptrollership Manual – Security Volume Chapter 6: *Storage of Sensitive Information and Assets*
- CBSA Comptrollership Manual – Security Volume Chapter 8: *Disposal of Sensitive Information and Assets*
- *CBSA Policy on the Use of Wireless Technology*
- *Customs Act*, s. 107
- D1-16-1 and D1-16-2
- Policy Guidelines on the Disclosure of Customs Information - Section 107 of the *Customs Act*
- EN Manual Pt7 Ch3
- CCTV Class of Records
- CCTV Personal Information Bank
- *CBSA Interim Video Review, Retention, Disclosure and Destruction Policy*
- MOU between Calgary International Airport and CBSA
- Video Recording and Monitoring Privacy Notice
- Video Surveillance Signage
- Audio and Video Signage
- Video Surveillance Sign Locations
- Privacy Notification given at interview rooms, primary inspection areas, secondary inspection areas and cash/information counters
- Inventory of Cameras
- PIA Action Plan
- TRA Summary
- TRA Action Plan
- Forensic Audio Video Analysis

SECTION 8 - FORMAL APPROVAL

The following signature represents a commitment to comply with sections 4 to 8 of the *Privacy Act* and the related privacy policy requirements outlined in the PIA as they relate to the administration of the identified program or activity.

Signature of PIA lead for program or activity

Date

Note: Responsibility for sections 4 to 8 of the *Privacy Act* rests with all employees of government institutions that handle personal information. Officials who manage such programs and activities are responsible for ensuring that such requirements are implemented as part of the administration of the program or activity.

The following signature represents a commitment by the Head of the institution or his/her delegate(s) who is responsible for establishing personal information banks in accordance with section 10 of the *Privacy Act*.

Signature of Head of the institution or the delegate responsible for Section 10 under the *Privacy Act*

Date

Note: Under the *Privacy Act*, the Head or his/her delegate(s) is responsible for complying with legal and relevant privacy policy requirements related to the approval and registration of personal information banks

Approval beyond the above sign-off should be inserted here :

(Signature of the title of the official)

OR

(Signature of the chair of the relevant governance committee)

Date

CBSA
PROTECTION • SERVICE • INTEGRITY

ASFC
PROTECTION • SERVICE • INTÉGRITÉ

Entry/Exit Wireless Handheld Device Privacy Impact Assessment (PIA)

Border Processing Unit
Traveller Transformation – Land Rail and Marine Division
Programs Branch



Name of Program / Activity / Service

PIA

Version Control

Version	Author	Action	Date
1	Renee Uvanile	Draft	April 18, 2017
2	Renee Uvanile	Input from ATIP	April 20, 2017
3	Renee Uvanile	Update to section 6 on guidance from ATIP.	April 24, 2017
4	Renee Uvanile	Input from Madona Radi	April 27, 2017
5	Maria Romeo	Comments (in track changes)	May 4, 2017
6	Renee Uvanile	Update regarding U.S. cellular	May 18, 2017
Final			

Stakeholders

Name	Role	Contact Information
Ron Warren	A/Manager, Border Processing Unit	Ron.Warren@cbsa-asfc.gc.ca 343-291-6145
Maria Romeo	Director	Maria.Romeo@cbsa-asfc.gc.ca
Robin Lortie	A/Manager, Corporate Affairs Branch	Robin.lortie@cbsa-asfc.gc.ca 343-291-6897
Neil O'Brien	Senior Policy Officer, ATIP	Neil.O'Brien@cbsa-asfc.gc.ca 343-291-6985
Steve Whittaker	Manager, Risk Assessment and Consultation	Steve.Whittaker@cbsa-asfc.gc.ca 343-291-6916

Table of Contents

VERSION CONTROL	2
STAKEHOLDERS	2
EXECUTIVE SUMMARY	6
ABBREVIATIONS AND ACRONYMS	7
DEFINITIONS	9
SECTION 1 - OVERVIEW AND INITIATION	10
SECTION 2 - RISK AREA IDENTIFICATION AND CATEGORIZATION	15
Type of Program or Activity	15
Type of Personal Information Involved and Context	15
Program or Activity Partners and Private Sector Involvement	17
Duration of the Program or Activity	17
Program Population	17
Technology and Privacy	18
Personal Information Transmission	19
Risk Impact to the CBSA	19
Risk Impact to the Individual or Employee	21
SECTION 3 - ANALYSIS OF PERSONAL INFORMATION ELEMENTS	22
SECTION 4 - FLOW OF PERSONAL INFORMATION	24
4.1 Data Flow Model - Diagram	24
4.3 Internal Use and Disclosure	27
4.4 External Use and Disclosure	27
4.5 Retention / Storage	28
4.6 Other Possible Considerations	29
SECTION 5 - PRIVACY COMPLIANCE ANALYSIS	30
1. Legal Authority for Collection of Personal Information	30
2. Necessity to Collect Personal Information	31
3. Authority for the Collection, Use or Disclosure of the Social Insurance Number	31
4. Direct Collection - Notification and Consent (as appropriate)	32
5. Indirect Collection - Consent or Authority under Sec. 10 of Privacy Regulations	33
6. Indirect Collection - Without Notification and Consent	34
7. Retention and Disposal of Personal Information	35
8. Accuracy of Personal Information	36
9. Use of Personal Information	37
10. Disclosures Directly Related to the Administration of the Program or Activity	38
11. Accounting for New Uses or Disclosures Not Reported in CBSA Info Source	40
12. Safeguards - Statement of Sensitivity	41
13. Safeguards - Threat and Risk Assessment	41
14. Safeguards - Administrative, Physical and Technical	42
15. Technology and Privacy - Tracking Technologies	43
16. Technology and Privacy - Surveillance or Monitoring	44
17. Considerations Related to Compliance, Regulatory Investigation, Enforcement ..	44
SECTION 6 - SUMMARY OF ANALYSIS AND RECOMMENDATIONS	47

SECTION 7 - SUPPLEMENTARY DOCUMENTS LIST	50
SECTION 8 - FORMAL APPROVAL.....	50
ANNEX A: PRIVACY COMPLIANCE CHECKLIST AND OTHER CONSIDERATIONS.....	51

Privacy Impact Assessment Date / Version:	YYYY-MM-DD (Date sent to OPC)
Office of the Privacy Commissioner file #:	
Project Implementation Plan (if applicable)	2017-04-18
Federal Institution:	Canada Border Services Agency (CBSA)
Related Class of Record Number:	CBSA ENF 129
Personal Information Bank:	CBSA PPU 1202
Government Official Responsible for PIA:	Vice President, Programs Branch
Delegate for section 10 of the <i>Privacy Act</i> :	ATI and Privacy Director, Dan Proulx

EXECUTIVE SUMMARY

Entry/Exit Wireless Handheld Devices

Wireless handheld devices will be introduced to support the Entry-Exit Initiative and Beyond the Border Action Plan. The devices will be equipped with a mobile version of the Integrated Primary Inspection Line (IPIL) application (i.e. mobile IPIL) to facilitate the secure and accurate capture and risk assessment of individual traveller and conveyance information. The devices will be deployed at Canada Border Services Agency (CBSA) service points which are not equipped with primary inspection booths. In addition, they will be deployed to ports of entry where primary inspection booths are present but do not support processing of all types of traveller processing. An example of this would be bus processing at large ports where workstations are only available in adjacent booths or buildings but not where officers process travellers directly. In this scenario, handheld devices will allow Border Services Officers (BSOs) to complete traveller processing on the bus rather than offloading passengers.

At most ports of entry, booths equipped with IPIL Air and Highway along with fixed workstations and document readers provide BSOs with a means of capturing traveller and conveyance (licence plate) information for risk assessment against customs and enforcement databases. Where no booth is available, BSOs must take licence plate and traveller information and run it at an IPIL workstation in an office adjacent to the primary inspection line. This forces the BSO to turn his/her back to the traveller and leave them unattended.

The introduction of handheld devices during primary processing will allow a BSO to capture and risk assess conveyance and traveller information while remaining with the traveller, just as they would today if they were working at a site with primary inspection booths.

This will increase security by providing BSOs with at hand access to information used in determining the travellers' admissibility. It will also streamline the entry process for our less automated ports and processes such as bus clearance. There will be no change to the type of information gathered today, only a change to the technology used to facilitate the collection.

At this time mobile devices are slated for deployment to 72 ports of entry and will be used to process travellers arriving via personal conveyance, bus, air and train. Deployment is starting at test sites (soft-launch) in June and then rolling out nationally in August 2017.

Protecting Your Personal Information

The following personal information elements related to the traveller will be handled by the wireless device:

Always	As Applicable
Name (First and Last)	Middle Name

Date of Birth	Document Number
Citizenship	Gender
	Results of previous enforcement
	eTA, Visa, TRBP number
	Membership (NEXUS, FAST etc.) information
	Photo TRB and NEXUS
	Licence Plate

While the mobile handheld device introduces a new means for capturing traveller and conveyance information, the type of data collected remains unchanged. Under normal circumstances there will be no traveller data stored on the device and information in transit will be encrypted with access limited to authorized users. The collection of information will be facilitated by handhelds.

The handheld is a tool used by the BSO to collect information directly from the traveller and verify it against information that is already held within CBSA information holdings. All information collected will be held within the CBSA's existing Integrated Customs System (ICS) platform. ICS is a common framework that encompasses both commercial and passenger-traveller streams and is comprised of a number of components (e.g. Passage History, Secondary Processing).

Right of Access

Individuals may formally request access to their personal information, or access to corporate records related to the wireless handhelds by filing a request with the Access to Information and Privacy Division. More information about this can be found on the Access to Information and Privacy page.

Accountability

Individuals with concerns about the collection, use, disclosure or retention of their personal information may issue a complaint to the CBSA Access to Information and Privacy Division. Complaints should be made in writing, and include the individuals name, contact information, and a brief description of their concerns. Contact the Access to Information and Privacy Division at the CBSA

ABBREVIATIONS AND ACRONYMS

ATIP	Access to Information and Privacy
BSO	Border Services Officer
CBSA	Canada Border Services Agency
COR	Class of Record
ESDC	Employment and Social Development Canada
eTA	Electronic Travel Authority
FA	Formal Arrangement

GOC	Government of Canada
GSP	Government of Canada Security Policy
IBAS	Integrated Border Alert System
ICS	Integrated Customs System
ICES	Integrated Customs Enforcement System
ID	Identification
IPIL	Integrated Primary Inspection Line
ISA	Information Sharing Agreement
LAC	Library and Archives Canada
MDM	Mobile Device Management
MOU	Memorandum of Understanding
MRZ	Machine Readable Zone
OGD	Other Government Department
OPC	Office of the Privacy Commissioner of Canada
PA	<i>Privacy Act</i>
PAXIS	Passenger Information System
PH	Passage History
PI	Personal Information
PIA	Privacy Impact Assessment
PIB	Personal Information Bank
PKD	Public Key Directory
PKI	Public Key Infrastructure
PNS	Privacy Notice Statement
PoE	Port of Entry
PSK	Pre Shared Key
SAR	Security Assessment Report
SOS	Statement of Sensitivity
SP	Secondary Processing
StatCan	Statistics Canada
TBS	Treasury Board Secretariat
TRA	Threat and Risk Assessment
TRB	Temporary Resident Biometric
VP	Vice-President
VPN	Virtual Private Network

DEFINITIONS

Action Plan	The Action Plan describes the steps that the Program will take to address risks that have been identified by ATI and Privacy Division, Office of the Privacy Commissioner of Canada (OPC) and Treasury Board Secretariat (TBS).
Administrative purpose	The <i>Privacy Act</i> defines an "administrative purpose" to be the use of an individual's personal information in a decision-making process that directly affects that individual.
Consistent use	Is a use that has a reasonable and direct connection to the original purpose(s) for which the information was obtained or compiled. This means that the original purpose and the proposed purpose are so closely related that the individual would expect that the information would be used for the consistent purpose, even if the use is not spelled out.
Data Matching	A comparison of personal data obtained from a variety of sources, including personal information banks, for the purpose of making decisions about the individuals to whom the data pertains. Data matching is a specialized activity involving the collection, use and disclosure of personal information that is subject to the various requirements of the <i>Privacy Act</i> .
Info Source	Is a series of annual TBS publications in which government institutions are required to describe their institutions, program responsibilities and information holdings, including PIBs and classes of personal information. The descriptions are to contain sufficient clarity and detail to facilitate the exercise of the right of access under the <i>Privacy Act</i> . Data-matching activities, use of the SIN and all activities for which privacy impact assessments were conducted have to be cited in <i>Info Source</i> PIBs, as applicable. The <i>Info Source</i> publications also provide contact information for government institutions as well as summaries of court cases and statistics on access requests.
Personal Information	Information about an identifiable individual as defined in section 3 of the <i>Privacy Act</i> . This definition, although lengthy, is not exhaustive, as indicated by the introductory phrase, "including, without restricting the generality of the foregoing". Information that is not specifically mentioned in the list may still be included in the definition of personal information if it qualifies as "information about an identifiable individual".
Personal Information Bank	Is a description of personal information that is organized and retrievable by a person's name or by an identifying number, symbol or other particular assigned only to that person. The personal information described in the personal information bank has been used, is being used, or is available for an administrative purpose and is under the control of a government institution.
Privacy	The OPC describes "privacy" as "... the right to control access to one's person and information about one's self. The right to privacy means that individuals get to decide what and how much information to give up, to whom it is given, and for what uses."
Mobile Device Management	Mobile Device Management (MDM) is a roles based service that will be leveraged to push policy to devices for standard configuration, provide remote support to devices, implement security controls and provide reports on usage and performance of mobile devices.

SECTION 1 - OVERVIEW AND INITIATION

Report Objectives

This report is a Privacy Impact Assessment (PIA) for the Entry/Exit wireless handheld devices. The introduction of wireless handheld devices will facilitate the secure and accurate capture and risk assessment of individual traveller and conveyance information at CBSA service points which are not equipped with primary inspection booths and in environments where traditional systems access is not readily available (such as bus processing).

The objectives of this PIA are:

- to review the business processes in order to identify the data flow of personal information;
- to analyze the collection, use, disclosure and retention of personal information;
- to determine if there are privacy risks associated with the introduction of mobile devices in primary processing; and
- to provide recommendations on the mitigation or elimination of the risks.

The information presented in this report follows the Treasury Board of Canada Secretariat (TBS) PIA policy and guidelines.

The purpose of a PIA process is to ensure that privacy is considered throughout the project development cycle. The results of a PIA are a documented guarantee that privacy issues have been identified and adequately addressed.

Government Institution: CBSA / Programs Branch

Government Official Responsible for the Privacy Impact Assessment

Martin Bolduc, Vice President, Programs Branch

Head of the government institution / Delegate for section 10 of the *Privacy Act*

Dan Proulx, Director, Access to Information and Privacy Division

Name of Program or Activity of the Government Institution:

This initiative relates to the 1.3 Admissibility Determination sub-activity and the 1.3.1 Highway Mode, 1.3.2 Air Mode, 1.3.3 Rail Mode and 1.3.4 Marine Mode sub-sub-activities.

Description of Program or Activity:

1.3 Admissibility Determination – through the Admissibility Determination program, the CBSA develops, maintains and administers the policies, regulations, procedures and partnerships that enable border services officers to intercept people and goods that are inadmissible to Canada, and to process admissible people and goods within established service standards. In addition, the Agency develops, maintains and administers the policies, regulations, procedures and partnerships to control the export of goods from Canada. In the traveller stream, border services officers question people upon arrival to determine if they and their personal goods meet the requirements of applicable legislation and regulations to enter Canada. Border services officers (BSOs) will then make a decision to grant entry or refer a person for further processing (e.g., payment of duties and taxes, issuance of a document), and/or for a physical examination.

1.3.1 Highway Mode - The Highway Program identifies and intercepts people and goods that are inadmissible to Canada seeking entry at 120 designated land ports of entry while ensuring that admissible people and goods are processed within established service standards. Border services officers conduct interviews of persons and drivers of commercial carriers and then make a decision to allow the entry of a person or shipment or refer them for further processing (e.g., payment of duties and taxes, issuance of a document) and/or examination (e.g., physical search of a vehicle, further investigation of admissibility).

1.3.2 Air Mode – The Air Program identifies and intercepts people and goods that are inadmissible to Canada seeking entry at designated airports while ensuring that admissible people and goods are processed within established service standards. Upon arrival, border services officers conduct interviews of persons seeking entry into Canada, aided by electronic pre-arrival risk-assessment information submitted by the airlines. CBSA officers make a decision to admit the person or refer them for further processing (e.g., payment of duties and taxes, issuance of a document) or examination. For private and corporate aircraft and general aviation traffic reporting through the Telephone Reporting Centre, various checks are conducted by means of the telephone reporting system. BSOs make a decision to admit people or refer them for further processing or examination. To assist border services officers in their examinations, detection tools such as detector dogs and ion scanners may be used. People and goods found to be in violation of the applicable legislation and/or regulations may be subject to a monetary penalty, seizure or denied entry to Canada.

1.3.3 Rail Mode - The Rail Program identifies and intercepts people and goods that are inadmissible to Canada seeking entry at a rail port of entry or rail yard while ensuring that admissible people and goods are processed within established service standards. Rail operators are required to report train, passenger and/or cargo information to the CBSA at or prior to arrival in Canada. Border services officers may conduct onboard interviews of travellers seeking entry into Canada upon arrival at the border to determine their admissibility or whether further processing (e.g., payment of duties and taxes, issuance of a document) or examination (e.g., physical search of baggage, further investigation of admissibility) is required.

In the commercial stream, border services officers review the electronic information submitted by the rail carrier and the importer/exporter, and make a decision to release the cargo or refer it for an examination at the rail yard.

1.3.4 Marine Mode - The Marine Program identifies and intercepts people and goods that are inadmissible to Canada seeking entry at a marine port of entry, while ensuring that admissible people and goods are processed within established service standards. Prior to arrival in the traveller stream, border services officers receive information regarding the passengers and crew aboard cruise ships, ferries, tour boats, private small vessels in the Trusted Traveller Program and commercial vessels. At large cruise ship offices and certain ferry terminals, passengers are processed using Integrated Primary Inspection Line. For those private vessels reporting through the Telephone Reporting Centre, various checks are conducted by means of the telephone reporting system. Border services officers make decisions to admit people or refer them for further processing or examination.

Description of the class of records associated with the program or activity:**Traveller Processing**

Description: Describes records related to people, goods and conveyances arriving at Canadian ports of entry. Specific to land mode only, records also include exit information (from Canada). May include records related to the establishment or use of electronic systems used to administer or manage the program.

Note : Records may be stored in the following systems: the *Integrated Customs Enforcement System (ICES)*, *Integrated Primary Inspection Line (IPIL)*, *Passenger Information System (PAXIS)*, *Telephone Reporting Centre System (TRCS)*, *Secondary Processing System (SP)*, *Passage History Database (PH)*, *Occurrence Reporting System (ORS)*, *Intelligence Management System (IMS)*, *Integrated Border Query (IBQ)*, *Field Operations Support System (FOSS)*, *Computer Assisted Immigration Processing System (CAIPS)*, *Canadian Police Information Centre (CPIC)*, *National Crime Information Center (NCIC)*, *Client Status Query (CSQ)*, *Modern War Crimes System (MWCS)*, *Secure Tracking System (STS)*, *Support System for Intelligence (SSI)*, *National Case Management System (NCMS)*, *Global Case Management System (GCMS)* and the *Automated Fingerprint Identification System (AFIS)*.

Document Types: Forms, manuals, policy, memoranda of understanding, passage and enforcement history.

Class of Record Number: CBSA ENF 129

- ☐ Proposal for a New Personal Information Bank
- ☐ Proposal to modify an existing Personal Information Bank - identify PIB registration number and current description:

Traveller Processing

Description: This bank describes information about individuals who enter Canada by way of a Canadian port of entry. This consists of persons - including pedestrians - aboard any personal or commercial conveyances, including crew. The personal information collected may include: name, contact information, citizenship, date of birth, place of birth, gender, date and time of entry, port of entry, travel document type (e.g., passport) including identification number and country of issuance, membership program information - i.e. NEXUS, residency, and Field Operations Support System (FOSS) ID number. In the land mode, passenger vehicle license plate information is collected.

Note: In addition to the requirements specified on the Treasury Board of Canada Secretariat Personal Information Request form, individuals requesting information described by this bank must provide the subject and date of examination at the border as well as the location of the port of entry. Bank formerly called *CIC PPU 001*.

Class of Individuals: General travelling public.

Purpose: The personal information is used in support of the administration of traveller processing activities. The personal information captured creates a passage history and allows the CBSA to initiate "real time" queries against enforcement actions and lookouts. Personal information is collected pursuant to *R41* and *R40* of the *Immigration and Refugee Protection Regulations*.

Consistent Uses: The information may be used or disclosed to assist CBSA's enforcement program, for program evaluation and for reporting purposes. The information may also be disclosed in support of domestic law enforcement and other partner agencies for the purpose of administration and enforcement of Acts of Parliament.

Retention and Disposal Standards: Records will be retained for six years plus the current year and then are destroyed.

RDA Number: 2006/004

Related Record Number: CBSA ENF 129

TBS Registration: 20110290

Bank Number: CBSA PPU 1101

Legal Authority for Program or Activity: Legal authority for the collection of personal information using wireless handheld devices is derived from multiple, inter-related legislations and regulations.

- o Information required from individuals as they request entry into Canada is derived from two legislations. 1) Section 11 of the *Customs Act*, which states, "every person arriving in Canada shall, except in such circumstances and subject to such conditions as may be prescribed, enter Canada only at a customs office designated for that purpose that is open for business and without delay present himself or herself to an officer and answer truthfully any questions asked by the officer in the performance of his or her duties under this or any other Act of Parliament." And 2) Section 18(1) of the *Immigration and Refugee Protection Act* which states, "Every person seeking to enter Canada must appear for an examination to determine whether that person has a right to enter Canada or is or may become authorized to enter and remain in Canada."

Program legislation as defined in the *Canada Border Services Act* "means any other Act of Parliament or any instrument made under it, or any part of such an Act or instrument,

(a) that the Governor in Council or Parliament authorizes the Minister, the Agency, the President or an employee of the Agency to administer and enforce, including the *Customs Act*, the *Customs Tariff*, the *Excise Act*, the *Excise Act, 2001*, the *Immigration and Refugee Protection Act* and the *Special Import Measures Act*;

(b) that the Governor in Council or Parliament authorizes the Minister, the Agency, the President or an employee of the Agency to enforce, including the *Agriculture and Agri-Food Administrative Monetary Penalties Act*, the *Canada Agricultural Products Act*, the *Feeds Act*, the *Fertilizers Act*, the *Fish Inspection Act*, the *Health of Animals Act*, the *Meat Inspection Act*, the *Plant Protection Act* and the *Seeds Act*;

(c) under which the Minister or another minister authorizes the Agency, the President or an employee of the Agency to administer a program or carry out an activity; or

(d) under which duties or taxes collected and paid pursuant to the *Customs Act* are imposed."

Summary of the initiative:

The introduction of handheld devices during primary processing will allow a BSO to capture and risk assess conveyance and traveller information while remaining with the traveller. The devices will have a mobile version of the Integrated Primary Inspection Line (IPIL) application (i.e. mobile IPIL) to facilitate the secure and accurate capture and risk assessment of individual traveller and conveyance information at CBSA service points which are not equipped with primary inspection booths and in environments where traditional systems access is not readily available (such as bus processing). The deployment of handhelds will introduce an additional tool in support of traveller processing and will not replace existing infrastructure at the port of entry.

The introduction of handhelds will increase security by providing BSOs with at hand access to information used in determining the travellers' admissibility. It will also streamline the entry process for our less automated ports and processes such as bus clearance. There will be no change to the type of information gathered today, only a change to the technology used to facilitate collection.

At this time, mobile devices are slated for deployment to 72 ports of entry and will be used to process travellers arriving via personal conveyance, bus, air, marine and train. Deployment is scheduled to begin in June 2017.

Eligible Travellers

All travellers arriving in Canada may have their information processed using a wireless handheld device.

Wireless Handheld Processing

When using a wireless handheld device, a BSO will approach a traveller or conveyance to obtain licence plate (as relevant) and traveller information. When processing a conveyance, licence plate information will be entered manually by the officer. Details from the travel documents will be read by the device using the Machine Readable Zone (MRZ) of the document or will be manually entered by an officer. Entry of conveyance and traveller details will initiate a risk assessment against CBSA systems and checks against relevant immigration databases. The results will be returned on the device to assist the officer in making his/her admissibility determination. The traveller will not interact with the device at any time.

Interaction with CBSA Officers

Travellers will be met by a BSO in the same manner that they are met today. Changes to processing may occur as follows:

Highway: Officer will complete primary processing with the traveller and will not leave them unattended. In bus processing, an officer may board the bus to complete primary processing.

Air: Officer may complete primary processing on the tarmac or on the aircraft.

Marine: Officer may complete primary processing on the dock or on the marine vessel.

Rail: Officer may complete primary processing on the train.

SECTION 2 - RISK AREA IDENTIFICATION AND CATEGORIZATION

Type of Program or Activity	Level of Risk
Program or activity that does NOT involve a decision about an identifiable individual	<input type="checkbox"/> 1
Administration of Programs / Activity and Services	<input checked="" type="checkbox"/> 2
Compliance / Regulatory investigations and enforcement	<input checked="" type="checkbox"/> 3
Criminal investigation and enforcement / National Security	<input checked="" type="checkbox"/> 4
Wireless handheld devices provide BSOs with a tool to collect the required personal information directly from the traveller for the determination of admissibility and the identification of any previous enforcement actions/lookouts. Traveller details will be encrypted and transmitted wirelessly via Government of Canada Wi-Fi or cellular connectivity.	

Type of Personal Information Involved and Context	Level of Risk
Only personal information, with no contextual sensitivities, collected directly from the	<input type="checkbox"/> 1

individual or provided with the consent of the individual for disclosure under an authorized program.

Personal information, with no contextual sensitivities after the time of collection, provided by the individual with consent to also use personal information held by another source. ☐ 2

Social Insurance Number, medical, financial or other sensitive personal information and/or the context surrounding the personal information is sensitive. Personal information of minors or incompetent individuals or involving a representative acting on behalf of the individual. ☒ 3

Sensitive personal information, including detailed profiles, allegations or suspicions, bodily samples and/or the context surrounding the personal information is particularly sensitive. ☐ 4

Details: Information is gathered from the traveller when a BSO manually enters their details or scans their travel document. This information is compared against information found in other CBSA information sources to determine whether or not the travellers are to be referred to Secondary for a more comprehensive examination. Specific data elements of the personal information will be limited to Biographic Entry Data and will or may include: Name (First/Given Name, Middle Name, Last Name/Surname), Date of Birth, Citizenship, Document number, Gender, Document Type, Licence Plate, photo. The SIN, medical, and financial information are not collected.

Program or Activity Partners and Private Sector Involvement

Level of Risk

Within the CBSA (amongst one or more programs within the CBSA)

☒ 1

With other federal institutions

☐ 2

With other or a combination of federal/ provincial and/or municipal government(s)

☐ 3

Private sector organizations or international organizations or foreign governments

☒ 4

Details: Primary inspection processing is completed by CBSA officials using a wireless handheld device. Traveller's information may be shared with other programs within the Agency via other lines of business separate from the handheld project.

Mobile device management allows for a small group of external security cleared individuals from the vendor to access the device remotely for the purpose of support. Measures have been put in place to ensure they will not be able to do so without the user of the device accepting the service. Users will be asked to ensure there is no personal information on the device screen when granting access which should not be problematic given support is not expected to occur during traveller processing.

Duration of the Program or Activity

Level of risk

One time program or activity

☐ 1

Typically involves offering a one-time support measure in the form of a grant payment as a social support mechanism.

Short-term program

☐ 2

A program or activity that supports a short-term goal with an established "sunset" date.

Long-term program

☒ 3

Existing program that has been modified or is established with no clear "sunset".

Details: The use of wireless handheld devices are a commitment under the Entry/Exit Initiative in support of the Beyond the Border Action Plan and are a long term commitment. Handheld devices are expected to support primary processing at locations where access to primary processing applications is limited for BSOs and traditional infrastructure would be too cumbersome or costly to put in place.

Program Population

Level of Risk

The program affects certain employees for internal administrative purposes.

☐ 1

The program affects all employees for internal administrative purposes.

☐ 2

The program affects certain individuals for external administrative purposes.

☒ 3

The program affects all individuals for external administrative purposes.

☐ 4

Details: This initiative affects individuals who present themselves at a port of entry where wireless handheld devices are being used. Given the devices are not used at all ports, many travellers arriving in Canada will not interact with handheld devices.

Technology and Privacy

- 6.1 Does the new or modified program or activity involve the implementation of a new electronic system, software or application program including collaborative software (or groupware) that is implemented to support the program or activity in terms of the creation, collection or handling of personal information? ☒ YES ☐ NO
- 6.2 Does the new or modified program or activity require any modifications to IT legacy systems and / or services? ☒ YES ☐ NO
- 6.3 Does the new or modified program or activity involve the implementation of one or more of the following technologies:
- 6.3.1 Enhanced identification methods: ☐ YES ☒ NO
 This includes biometric technology (i.e. facial recognition, gait analysis, iris scan, fingerprint analysis, voice print, radio frequency identification (RFID), etc...) as well as easy pass technology, new identification cards including magnetic stripe cards, "smart cards" (i.e. identification cards that are embedded with either an antenna or a contact pad that is connected to a microprocessor and a memory chip or only a memory chip with non-programmable logic).
- 6.3.2 Use of Surveillance: ☐ YES ☒ NO
 This includes surveillance technologies such as audio/video recording devices, thermal imaging, recognition devices, RFID, surreptitious surveillance / interception, computer aided monitoring including audit trails, satellite surveillance etc.
- 6.3.3 Use of automated personal information analysis, personal information matching and knowledge discovery techniques: ☒ YES ☐ NO
 For the purposes of the Directive on PIA, CBSA is to identify those activities that involve the use of automated technology to analyze, create, compare, cull, identify or extract personal information elements. Such activities would include personal information matching, record linkage, personal information mining, personal information comparison, knowledge discovery, information filtering or analysis. Such activities involve some form of artificial intelligence and/or machine learning to uncover knowledge (intelligence), trends/patterns or to predict behaviour.

Details: Information gathered with wireless handheld devices will be utilized by the CBSA in the same manner that it is used today. This includes: matching that information to enforcement and immigration records and storing it to passage history to create a record of entry. A mobile version of the CBSAs IPIL application was developed to support this activity on a handheld device. This information may be used by the Agency at a later date to uncover knowledge or identify patterns/trends.

In addition to a mobile version of IPIL, Mobile Device Management is being introduced but will not be used to create, collect or handle personal information.

Passage history which is a legacy system will be modified to identify that a passage was processed using a mobile device.

No biometrics will be gathered using the device. While there is a camera on the device it is disabled and will not be available for use by the officer.

No surveillance will take place.

Personal Information Transmission

Level of Risk

- | | |
|--|---------------------------------------|
| The personal information is used within a closed system.
No connections to Internet, Intranet or any other system. Circulation of hardcopy documents is controlled. | <input type="checkbox"/> 1 |
| The personal information is used in system that has connections to at least one other system. | <input checked="" type="checkbox"/> 2 |
| The personal information is transferred to a portable device or is printed.
USB key, CD-Rom, laptop computer, any transfer of the personal information to a different medium. | <input type="checkbox"/> 3 |
| The personal information is transmitted using wireless technologies. | <input checked="" type="checkbox"/> 4 |

Details: Traveller information is used in the Mobile IPIL application which interfaces with the following systems:

- The Integrated Customs System (ICS) for storage of records in passage history.
- The Integrated Customs Enforcement System (ICES) a CBSA system which holds customs enforcement records.
- The Integrated Border Alert System (IBAS) a CBSA system which holds immigration data.
- The mobile device management system which allows CBSA IT and Security to control device policy, remotely access and administer security measures on the devices.

Information is encrypted and transmitted wirelessly via an approved Government of Canada Wi-Fi solution with encrypted cellular connectivity as a backup. In addition, due to lack of physical infrastructure at a limited number of locations only encrypted cellular services will be leveraged. A diagram outlining the connectivity is provided in section 4.

Risk Impact to the CBSA

Level of Risk

Entry/Exit Wireless Handhelds	PIA
Managerial harm.	<input type="checkbox"/> 1
Processes must be reviewed, tools must be changed, change in provider / partner.	
Organizational harm.	<input type="checkbox"/> 2
Changes to the organizational structure, changes to the organizations decision-making structure, changes to the distribution of responsibilities and accountabilities, changes to the program activity architecture, departure of employees, reallocation of HR resources.	
Financial harm.	<input type="checkbox"/> 3
Lawsuit, additional moneys required reallocation of financial resources.	
Reputation harm, embarrassment, loss of credibility.	<input checked="" type="checkbox"/> 4
Decreased confidence by the public, elected officials under the spotlight, institution strategic outcome compromised, government priority compromised, impact on the Government of Canada Outcome areas.	

Details: In the event of a breach of the personal information collected and transmitted by the handhelds, there would be a decrease in public confidence regarding the CBSA's ability to responsibly handle personal information. In most circumstances, data will not be stored on the device thereby limiting the possibility of breach. In addition, safeguards are in place to protect information including encryption of data. Note that United States Customs and Border Protection (U.S. CBP), the Royal Canadian Mounted Police (RCMP) and Canada Post securely leverage mobile services within their operation.

Risk Impact to the Individual or Employee	Level of Risk
Inconvenience.	<input checked="" type="checkbox"/> 1
Reputation harm, embarrassment.	<input checked="" type="checkbox"/> 2
Financial harm.	<input checked="" type="checkbox"/> 3
Physical harm.	<input type="checkbox"/> 4

Details: In the event of a breach of personal information collected and transmitted by the handheld, there could be the possibility of identity theft of the individual. Again, security measures have been put in place to mitigate this risk.

Entry/Exit Wireless Handhelds

PIA

SECTION 3 - ANALYSIS OF PERSONAL INFORMATION ELEMENTS

The following table lists the personal information elements collected via the wireless handheld.

All Transactions					
Category Of Personal Information	Personal Information Element	Personal Information Sub-Element	Format	Source	Purpose / Necessity of Element
Name	Name	1) Last name, first name,	Electronic	Derived from the travel document	To document border crossing; identify travellers in existing CBSA information holdings and assess admissibility.
Date of birth	Date of birth	1) Day of birth 2) Month of birth 3) Year of birth	Electronic	Derived from the travel document	To identify travellers in existing CBSA information holdings and assess admissibility.
Citizenship / Nationality	Citizenship / Nationality	1) Citizenship / nationality of traveller	Electronic	Derived from the travel document or entered manually by officer.	To document border crossing; identify travellers in existing CBSA information holdings and assess admissibility.
Some Transactions					
Gender	Gender	Gender of Traveller	Electronic	Derived from the travel document or entered manually by officer.	To identify travellers in existing CBSA information holdings.
Travel Document Information (may be their Passport)	Travel Document Information	1) Document Type 2) Document Number 3) Document Country of Issuance 4) Document expiration date	Electronic	Derived from the travel document or entered manually by officer.	To document border crossing; identify travellers in existing CBSA information holdings and assess admissibility; to verify the validity and authentication of the travel document. In the past, a CBSA officer would manually verify the travel document.
Name	Name	Middle Name	Electronic	Derived from the travel document or entered manually by officer.	To document border crossing; identify travellers in existing CBSA information holdings and assess admissibility.

Entry/Exit Wireless Handhelds

PIA

Licence Plate	Licence plate number and province/state	1)Number 2)Province/state	Electronic	Entered manually by officer.	To document border crossing; identify conveyances in existing CBSA information holdings and assess enforcement history.
eTA, VISA, TRB Information	Document number	eTA: whether on file VISA: whether on file TRB: photo, document number	Electronic	Retrieved from back end database.	To determine if immigration requirements have been met.
Risk Assessment Results	Information related to previous enforcement.	Information related to previous customs, immigration or criminal enforcement activity.	Electronic	Retrieved from back end database.	To determine if secondary examination is required.
Membership (NEXUS Fast etc.) Information	Membership status (expired etc.), photo and number.	Membership status (expired etc.), photo and number.	Electronic	Retrieved from back end database.	To determine if immigration requirements have been met.

SECTION 4 - FLOW OF PERSONAL INFORMATION

Diagram 1

The following diagram has been included to show information flow in the operational context. The infrastructure has been simplified for this purpose.

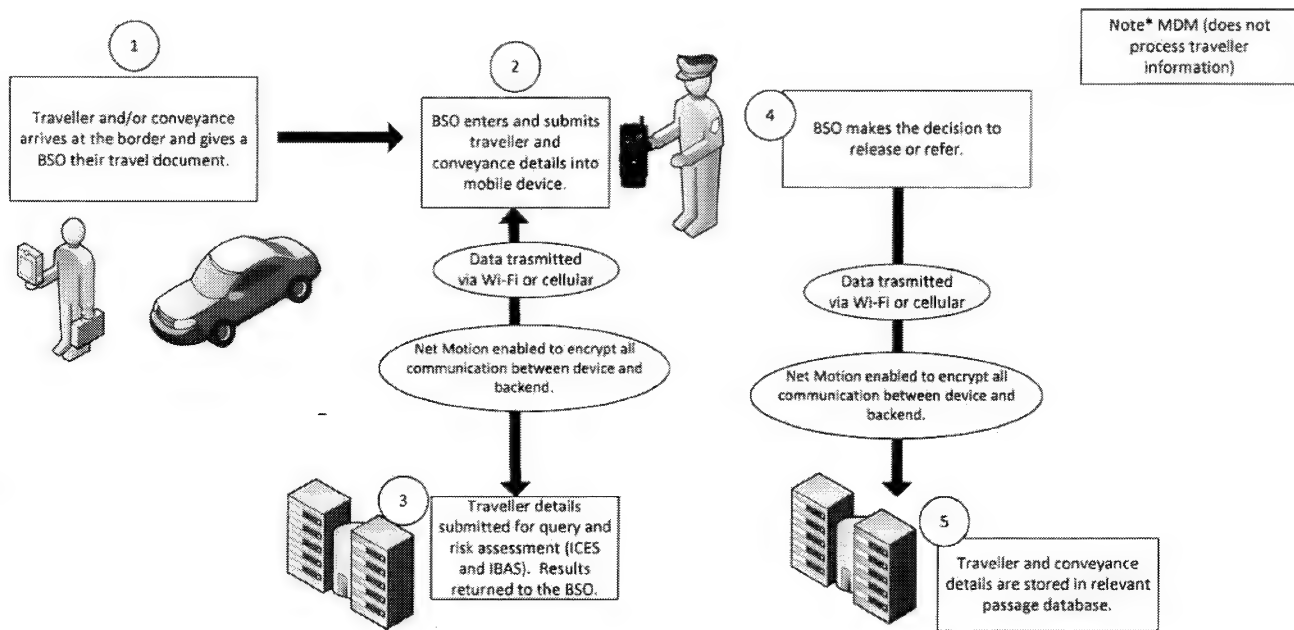


Diagram 2

The following diagram is an overview of the respective components/services which will be leveraged for supporting the infrastructure the Entry/Exit hand held project is dependent upon. The **PILSERVICESYNC** service has been added for reference only. Its inclusion is intended to depict the eventual connectivity requirement. **MDM Services** for device management.

Netmotion Services for secure connectivity.

Active Directory (AD) Services for secure auditable device authentication.

Malware/Intrusion Detection System/Patch Management Services for alignment of new infrastructure with existing security safeguard mechanisms.

Monitoring Services for alignment of new infrastructure with existing monitoring/alert mechanisms.

Network Services leveraging of both existing services and newly implemented GC Wifi services.

PILSERVICESYNC Services for reference to target business risk assessment services.

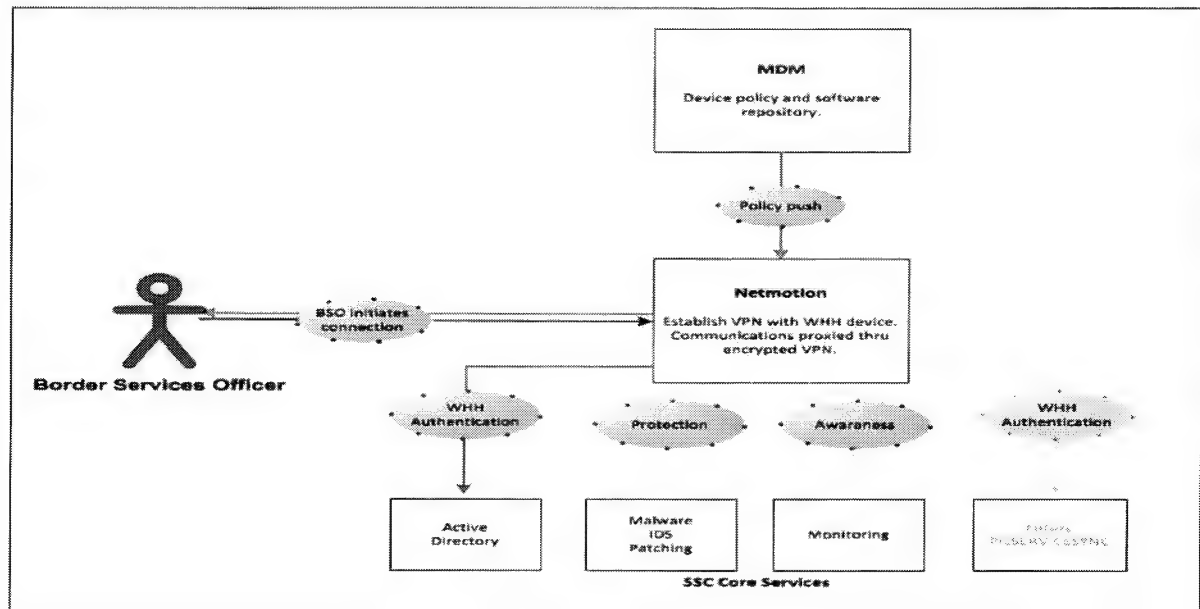
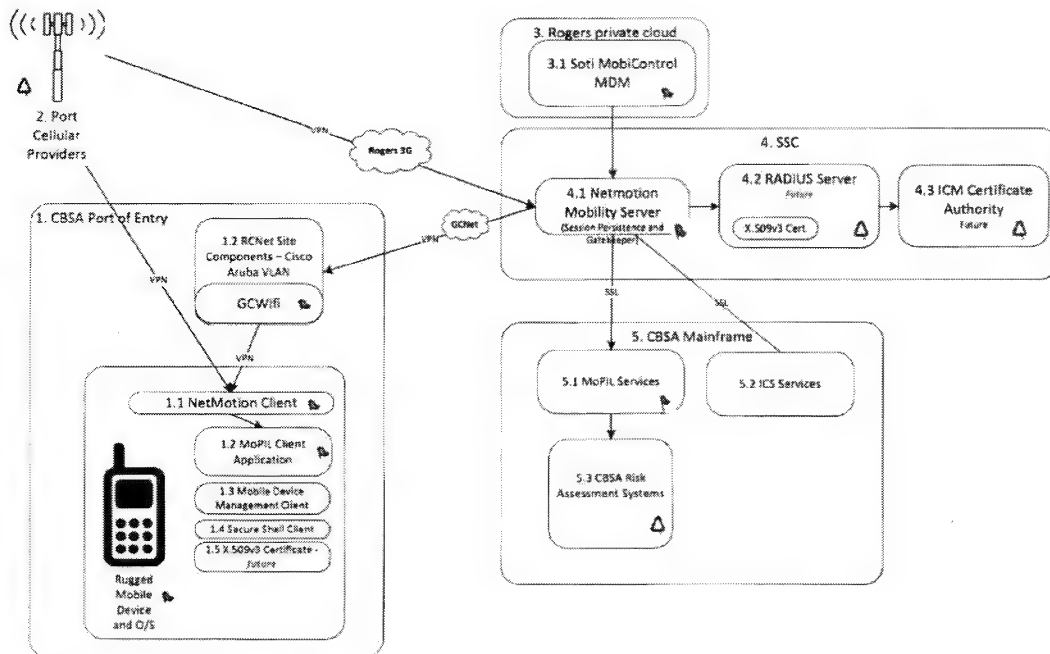


Diagram 3

This service will leverage the current Government of Canada (GC) Wi-Fi service with cellular as back up in most cases and cellular as the main connectivity type at a few locations. The GC Wi-Fi service has been configured in such a fashion as to provide Wi-Fi coverage which meets identified CBSA areas of operations. MDM services will provide device security and standardization via SOTI MobiControl services. Device policies will lock down the device function to application use only, provide locational services, reporting, and allow the CBSA to remotely manage the fleet of devices. Net motion services will permit secure connection of the data via an encrypted tunnel. Connectivity will be supported from both GC Wi-Fi and cellular connections. Net motion adds an additional level of security to the remote PIL function by encrypting the data in motion.



2 Data Flow Model - Table

SOURCE	IDENTIFY THE SOURCE
The individual or a representative	A traveller or their legal representative may request their own information.
CBSA Information Holdings	<p>CBSA Information holdings such as:</p> <ul style="list-style-type: none"> • Integrated Customs System (ICS): An umbrella system used for storage of traveller details to account for passage history— CBSA PPU 008. • Integrated Custom Enforcement System (ICES) – CBSA PPU 016. Data from the following programs is accessed through ICES: <ul style="list-style-type: none"> ○ Criminal Investigation Program – CBSA PPU 1402; and ○ Intelligence Program – CBSA PPU 035. • Interdiction and Border Alert System (IBAS). Data from the following programs/systems is retrieved through IBAS: <ul style="list-style-type: none"> ○ Immigration Investigations Program – CBSA PPU 1403 ○ Enforcement Information Index System (EIIS) – CBSA PPU 025 ○ Document Integrity Program – CBSA PPU 1404 <p>The Lost Stolen Fraudulent Document (LSFD). *Immigration related data is retrieved from Global Case Management System (GCMS) through IBAS.</p>
Royal Canadian Mounted Police Information Holdings	A subset of Wants and Warrants from Canadian Police Information Centre (CPIC) is sent to ICES (CBSA PPU 016).

4.3 Internal Use and Disclosure

Program	Personal information bank
N/A	

4.4 External Use and Disclosure

The individual or a representative	An individual or their representative may request their own personal information.
A federal government institution	N/A
- Provincial Government	N/A
- Municipal Government	N/A
- Aboriginal Government / Council	N/A
- Organization of a Foreign State	N/A
- International Organization	N/A
- Located in Canada and Canadian Owned	No systematic use or disclosure of personal information.
- Located in Canada and Foreign Owned	No systematic use or disclosure of personal information.
- Located abroad and Canadian Owned	No systematic use or disclosure of personal information.
- Located abroad and Foreign Owned	No systematic use or disclosure of personal information.

4.5 Retention / Storage

Canada Border Services Agency - Integrated Customs System (ICS), Passage History database	Files are retained for seven years from the date of the traveller's entry to Canada, as identified by the traveller's passage time, recorded by the device. This reflects existing retention periods for traveller processing. After this period, the records are destroyed.
---	--

4.6 Other Possible Considerations

Identify Groups or Areas / or Divisions	Positions who have access or use the personal information (where appropriate)	Geographical Location
The CBSA responsible for program or activity:		
Information, Science and Technology Directorate	Approximately 20-25 staff members in a production support role, responsible for receiving incidents and requests from end-users, analyzing these and either responding to the end user with a solution or escalating it to the other IT teams. These teams may include developers, system engineers and database administrators handling system issues.	National Capital Region
Border Operations Directorate	Border Services Officers, interns/students, Superintendents, Chiefs of Operations at ports of entry where handhelds will be deployed.	National
Other federal government Institution responsible for program or activity:		
N/A		

SECTION 5 - PRIVACY COMPLIANCE ANALYSIS

1. Legal Authority for Collection of Personal Information

Has a legal authority been identified for the collection of personal information for this program or activity?

Yes

- 1.1 ☒ Specify the legal authority and briefly explain its connection to the program or activity or how it permits the collection of the personal information:

Legal authority for the collection of personal information is derived as follows:

- o Information required from individuals as they request entry into Canada is derived from two legislations. 1) Section 11 of the *Customs Act*, which states, "every person arriving in Canada shall, except in such circumstances and subject to such conditions as may be prescribed, enter Canada only at a customs office designated for that purpose that is open for business and without delay present himself or herself to an officer and answer truthfully any questions asked by the officer in the performance of his or her duties under this or any other Act of Parliament." And 2) Section 18(1) of the *Immigration and Refugee Protection Act* which states, "Every person seeking to enter Canada must appear for an examination to determine whether that person has a right to enter Canada or is or may become authorized to enter and remain in Canada."

Program legislation as defined in the Canada Border Services Act "means any other Act of Parliament or any instrument made under it, or any part of such an Act or instrument,

(a) that the Governor in Council or Parliament authorizes the Minister, the Agency, the President or an employee of the Agency to administer and enforce, including the *Customs Act*, the *Customs Tariff*, the *Excise Act*, the *Excise Act, 2001*, the *Immigration and Refugee Protection Act* and the *Special Import Measures Act*;

(b) that the Governor in Council or Parliament authorizes the Minister, the Agency, the President or an employee of the Agency to enforce, including the *Agriculture and Agri-Food Administrative Monetary Penalties Act*, the *Canada Agricultural Products Act*, the *Feeds Act*, the *Fertilizers Act*, the *Fish Inspection Act*, the *Health of Animals Act*, the *Meat Inspection Act*, the *Plant Protection Act* and the *Seeds Act*;

(c) under which the Minister or another minister authorizes the Agency, the President or an employee of the Agency to administer a program or carry out an activity; or

(d) under which duties or taxes collected and paid pursuant to the *Customs Act* are imposed."

- 1.3 ☒ Is the personal information collected directly related to an operating program or activity?

Yes it is related to the admissibility program.

No

- 1.3 ☐ If there is no legal authority for the collection of personal information, it cannot be collected. Please consult your legal advisor to determine if there is authority to proceed with the program or activity.

2. Necessity to Collect Personal Information

Is each element and sub-element of personal information collected or to be collected necessary to administer the program or activity?

YES

- 2.1 ☒ Ensure that all personal information necessary to administer the program or activity is listed in the relevant PIB.
- 2.2 ☒ AND, implement controls and procedures to ensure the CBSA does not collect more personal information than is necessary for the identified program or activity and that a continuing need exists for that information or its collection.

2.3 Are secondary uses contemplated for the information collected?

☒ YES ☐ NO

The use of the information for enforcement (if required) is internal to the CBSA and disclosures to other government departments as required and permitted by law. These uses are documented in the Personal Information Bank.

2.3.2 If not, is there authority for the use or disclosure of the personal information?

☐ YES ☐ NO

NO

- 2.3 ☐ Review the proposed elements and sub-elements of personal information outlined in "Section 3 – Analysis of Personal Information Elements" to identify those that are "necessary" and not merely useful. Document any changes.

3. Authority for the Collection, Use or Disclosure of the Social Insurance Number

Is the collection of the Social Insurance Number (SIN) necessary to administer the program or activity?

YES

- 3.1 ☐ Collection of the SIN must be in compliance with the *Directive on Social Insurance Number* (please check all appropriate boxes below):

3.2 ☐ State legal authority for collecting the SIN:

OR, in the absence of a legal authority to collect the SIN:

3.3 ☐ Establish explicit authority through legislative amendment(s).

3.4 ☐ Establish legal authority as outlined in the *Directive on Social Insurance Number*.

AND, if disclosure of the SIN by the CBSA is to occur on a routine or systematic basis

3.4.1 ☐ to another federal institution that is authorized to collect it, or to another level of government, establish an agreement or arrangement that includes specific provisions to limit the use of the SIN.

3.4.2 ☐ to a contractor or other external service provider, establish a contract that includes specific provisions to limit the use of the SIN.

3.5 ☐ AND, ensure that the relevant **PIB** for the program or activity states the authority under which the SIN is collected and the purpose for which it is used.

NO

3.6 ☒ The SIN is not necessary and it will not be collected, used or disclosed to administer the program or activity.

4. Direct Collection - Notification and Consent (as appropriate)

Is personal information collected directly from the individual to whom it relates?

YES

- 4.1 ☐ A "Privacy Notice" (adapted for either verbal or written communications) must be provided to the individual at the time of collection and it must include the following elements:
- a) The purpose and authority for the collection
 - b) Any uses or disclosures that are consistent with the original purpose.
 - c) Any uses or disclosures that are not related to the original purpose
 - d) Any legal or administrative consequences for refusing to provide the personal information
 - e) That the "individual to whom the information relates" has rights of access to, correction of and protection of personal information under the *Privacy Act*.
 - f) A reference to the **PIB** for the program or activity
 - g) Why the SIN is collected, how it will be used and the consequence of not providing it.

AND, add a "Consent Statement" to the "Privacy Notice" as appropriate, if the personal information is to be used or disclosed for a purpose other than the original purpose (**Secondary Use**) or a consistent use, or, to authorize indirect collection of personal information.

- 4.2 ☐ The "Consent Statement" must include the following elements:
- a) The purpose of the consent and the specific personal information involved.
 - b) In the case of indirect collections, the sources that will be asked to provide the information.
 (This element need only be included when personal information is to be collected from another source e.g., person or organization with the consent of the individual)
 - c) Uses and disclosures that are not consistent with the original purpose of the collection and for

which consent is being sought.

(This element need only be included when the individual's consent is sought for a secondary use or disclosure that is not consistent with the original purpose for which the information is collected. To find out if the individual's consent is necessary for such a use or disclosure, please consult the ATI and Privacy Division)

- d) Any consequences that may result from withholding consent.
- e) Any alternatives to providing consent

- 4.3 ☐ AND, implement controls and procedures to ensure that the CBSA keeps a record documenting whether or not an individual provided consent when it was sought, including a record documenting any withdrawal of consent when applicable.

****Ensure to provide the "controls and procedures" as an annex to this PIA****

Additional Consent Considerations (s. 77(1)(m) of the *Privacy Act*):

- ☐ Standards and mechanisms are in place to ensure that the individual has capacity to give consent.

****Ensure to provide the "standards and mechanisms" as an annex to this PIA****

NO

- 4.4 ☐ The personal information necessary for the program or activity is not collected directly from the individual. It is collected indirectly, for example, from another program within the CBSA, or from another institution, government or third party.

5. Indirect Collection - Consent or Authority under Sec. 10 of Privacy Regulations

Is personal information collected indirectly from another source with the informed consent of the individual to whom it relates, or from a person authorized to act on behalf of the individual pursuant to section 10 of the Privacy Regulations?

YES

- 5.1 ☐ The notice and consent requirements stated at Question 4 apply. Please provide the "**Privacy Notice**" and/or "**Consent Statement**" below:

****For a copy of the CBSA Privacy Notice and Consent Statement template, contact the ATI and Privacy Division****

- 5.2 ☐ AND, implement controls and procedures to ensure the CBSA keeps a record documenting whether or not an individual provided consent when it was sought, including a record documenting any withdrawal of consent when applicable.

****Ensure to provide the "controls and procedures" as an annex to this PIA****

- 5.3 ☐ AND, if information is being collected from persons authorized to act on behalf of minors, incompetents or individuals who have been deceased for less than 20 years, implement appropriate mechanisms to ensure that such persons are authorized to act on behalf of individuals who do not have the capacity to provide consent.

****Ensure to provide the "mechanisms" as an annex to this PIA****

NO

5.4 ☒

The information collected via wireless handheld device is collected directly.

6. Indirect Collection - Without Notification and Consent

Is personal information collected from another source without notice to or consent from the individual to whom the information relates?

YES

6.1 ☐ Where information is collected indirectly under any of the following circumstances without notice to, or consent from, the individual to whom it relates, please check the applicable boxes and explain as requested:

☐ a) The collection is a result of a disclosure to the CBSA under subsection 8(2) of the *Privacy Act*. State the applicable paragraph(s) of subsection 8(2) and provide a brief explanation for each:

Details: *(This information is mandatory)*

☐ b) Direct notification of the individual might result in the collection of inaccurate information, or might defeat the purpose or prejudice the use for which the information is collected. Briefly explain why notice is not provided: (For example, certain kinds of lawful investigation might be jeopardized if the investigators were required to notify the individuals who were the subjects of the investigations before collecting information indirectly from other sources.)

Details: *(This information is mandatory)*

☐ c) The information involved in the program or activity is to be used solely for a non-administrative purpose in which no decisions are made about the individuals to whom the information relates. (This includes research, statistical, audit or evaluation purposes.)

6.2 ☐ AND, if any of the circumstances in a) b) or c) is applicable, ensure that it is reflected in the relevant **PIB**.

6.3 ☐ AND, if the information is to be used solely for a non-administrative purpose (box c above has been checked), ensure that the requirements under sections 6.3.2 and 6.3.3 of the *Directive on Privacy Impact Assessment* have been met, and that the decision of the official responsible for section 10 of the *Privacy Act* to proceed with a CBSA PIA for the program or activity has been adequately documented in the description of the program or activity in "Section 1 - Overview and PIA Initiation" of the CBSA PIA.

6.4 ☐ OR, if none of the circumstances in a) b) or c) is applicable, then the personal information must be collected directly from the individual, or indirectly with the consent of the individual. Please review the responses to Questions 4 and 5 and ensure that the "Privacy Notice" or the "Consent

Statement" includes all of the required elements within Question 4.

NO

- 6.5 ☒ All personal information is collected directly from the individual to whom it relates, or from another source with notice to, or consent from, the individual or a person authorized to act on behalf of the individual.

7. Retention and Disposal of Personal Information

Has Library and Archives Canada approved a records retention and disposal schedule that applies to the personal information?

YES

- 7.1 ☒ Please identify the Record Disposition Authority (RDA) and describe the retention and disposal schedule:
- 7.2 ☒ AND, implement controls and procedures to ensure that personal information used to make a decision that directly affects an individual will be retained for a minimum of two years after the last administrative action or, where a request for access to the information has been received, until such time as the individual has had the opportunity to exercise all his/her rights under the Act.
- 7.3 ☐ AND, if the CBSA intends to dispose of personal information that has been used for an administrative purpose prior to the expiration of the two-year minimum retention standard established by the *Privacy Regulations*, it must obtain the consent of the individual to whom the information relates before doing so.
- 7.4 ☒ AND, the CBSA must cite the RDA number, the retention period and the disposition standards for the personal information in the relevant **PIB**.

Details: The RDA listed in the PIB is 2000/033, which is an active Records Disposition Authority confirmed through the Library and Archives Records Disposition Authorities Control System. While the terms and conditions list only the Customs Branch of the Canada Customs and Revenue Agency, the authorization portion of the RDA listing includes records collected or held by the CBSA.

The RDA terms and conditions are generic in nature, requesting only that records that are considered to have archival value be transferred to LAC and enable the CBSA to set the required retention period and related destruction for records that are not archival in nature.

The retention period for information collected via the handheld will be aligned with the retention period for passage history (i.e., seven years).

NO

- 7.5 ☐ Provide a Records Disposition Submission to Library and Archives Canada describing the records containing the personal information for which the institution requires a RDA.

- 7.6 ☐ AND, obtain a RDA from Library and Archives Canada to allow the CBSA, under certain conditions, to dispose of records that no longer have operational utility for the program or activity.
- 7.7 ☐ AND, ensure that all the other applicable requirements listed under "YES" at Question 7 are met.

8. Accuracy of Personal Information

Will measures be adopted to ensure that personal information used by the CBSA for an administrative purpose is as accurate, up-to-date and complete as possible?

YES

8.1 Please check any of the following measures that will be adopted to ensure accuracy of the personal information and provide details as requested:

- 8.1.1 ☒ Personal information will be collected directly from the individual to whom it relates or it will be validated with the individual or a person authorized to act on behalf of the individual.
- 8.1.2 ☒ A data-matching process will be used to verify the accuracy of personal information against a "reliable source" (within or outside the CBSA) where this is authorized, or where consent was obtained.
- 8.1.3 ☐ In cases where direct collection or consent is not feasible, the CBSA will obtain information from trusted sources (public or private) and verify accuracy against existing personal information before use.
- 8.1.4 ☒ Technological methods will be used to identify errors and discrepancies.
- 8.1.5 ☐ Other
- 8.2 ☐ AND, if measures are adopted other than "direct collection or validation with the individual or with a person authorized to act on behalf of the individual", the CBSA must implement appropriate controls and procedures to ensure that:
- a) the technique(s) and the specific source(s) used to validate or update the personal information are documented;
 - b) individuals are given the opportunity, whenever possible, to request correction of any inaccurate personal information before the information is used in a decision-making process that affects them;
 - c) personal information can only be modified or corrected by those within the CBSA who have the authority to do so;
 - d) when personal information is corrected or annotated, the record of personal information indicates the date of the last correction or annotation and the source of the information used to make the correction or annotation; and
 - d) when personal information is corrected or annotated, other authorized holders of the information are notified about the correction or annotation and that all copies of the information in the possession of the CBSA are corrected / annotated.
- 8.3 ☐ AND, if appropriate, ensure that the "Privacy Notice" or "Consent Statement" and the relevant **PIB** are amended to identify the data-matching activity including the source(s).

Details:

To minimize errors technologies that provide the capacity to electronically capture traveller details from documents have been included in the device. This includes MRZ, barcode and mag stripe reading.

Personal information collected with the handheld will be verified through querying existing CBSA information holdings, such as: Customs Enforcement System (ICES) and Interdiction and Border Alerting System (IBAS). Discrepancies may result in a referral to secondary processing.

NO

8.4 ☐

Explain why such measures will not be adopted: *(This information is mandatory)*

9. Use of Personal Information

Will the personal information collected for the program or activity be used solely for the original purpose for which it was obtained or compiled, a use consistent with that purpose, or a purpose for which the information was disclosed to the institution pursuant to subsection 8(2) of the Privacy Act?

YES

- 9.1 ☒ Implement controls and procedures to ensure that access to the personal information for such purposes will be limited to authorized individuals who need to know the information to perform their official duties.

Details: Access to and use of all traveller information is controlled using roles based system permissions granted on a need to know basis. Those granted permission to access the information can only do so using a valid user name and password.

- 9.2 ☒ AND, ensure that the "Data Flow Diagram" or "Data Flow Tables" completed for "Section 4 – Flow of Personal Information" of the CBSA PIA identify the areas, groups and individuals (e.g., the positions) within the CBSA who have a need-to-know to access to or handle the personal information, including their geographical location and where the personal information will be stored or retained.

- 9.3 ☒ AND, if the purposes for which the personal information is used includes any use(s) of the information for a non-administrative purpose, (such as research, statistical, audit and evaluation purposes) the CBSA will adhere to the requirements and principles in the **CBSA Privacy Protocol For Non-Administrative Purposes** (2012), in accordance with section 6.2.15 of the *Policy on Privacy Protection*, to address any impact that such non-administrative uses may have on privacy.

NO

- 9.4 ☐ Identify below any other uses of the personal information, in other words, any routine uses that are

not directly related to the purpose of the collection, or, which are not consistent with that purpose or for which the information was disclosed to the CBSA pursuant to subsection 8(2) of the *Privacy Act*:

Detail : *(This information is mandatory)*

- 9.5 ☐ AND, ensure that these other uses are reflected in the relevant **PIB**. (In accordance with subsection 9(1) of the *Privacy Act*, if these other uses are not described in the PIB in CBSA Info Source, the CBSA is required to record each use on the individual's file. Describing them in the PIB is, therefore, a far more efficient practice – see Question 11.)
- 9.6 ☐ AND, include a description of these other uses in the "**Privacy Notice**" or "**Consent Statement**", as appropriate,
- ☐ AND, ensure the all the other applicable requirements listed under "**YES**" at Question 9 are met.

10. Disclosures Directly Related to the Administration of the Program or Activity

Will personal information be disclosed for purposes directly related to the administration of the program or activity?

YES

- 10.1 ☒ Please check all applicable boxes below and, for each disclosure, identify the name of the organization or third party to which personal information will be disclosed. If it is disclosed within the CBSA, please identify the branch and the program or activity.

- 10.1.1 ☐ Within the CBSA for another program or activity

Details:

- 10.1.2 ☐ Other federal government institutions

Details:

- 10.1.3 ☐ Provincial, territorial or municipal governments institutions

- 10.1.4 ☒ Foreign government institutions and entities thereof

Details: Information will be shared in accordance with the Entry/Exit PIA.

- 10.1.5 ☐ International organizations

- 10.1.6 ☐ The private sector (e.g., contractor or other external service provider)

- 10.1.7 ☐ Other

- 10.2 ☒ AND, ensure that:

- a) any such disclosure is made in compliance with section 8 of the *Privacy Act*, which allows disclosures of personal information with consent of the individual to whom the information relates (subsection 8(1)) or without consent in certain and limited circumstances pursuant to subsection 8(2) of the Act;

- b) only personal information elements that are necessary for the intended purpose are disclosed;
- c) the organization or third party receiving the personal information is authorized to do so;
- d) administrative, physical and technical safeguards appropriate to the sensitivity of the information will be applied to protect the information during and after its transmission (see Question 15);
- e) the organization or third party to which the personal information will be disclosed for the administration of the program or activity are identified in the "Consistent Use" section in the relevant **PIB** in *CBSA Info Source*, including the specific purpose of the disclosure;
 the "Privacy Notice" or "Consent Statement" describes any disclosures of information;
- f) the "Data Flow Diagram" or "Data Flow Tables" completed in "Section 4 – Flow of Personal Information" of the CBSA PIA include details on the disclosed personal information:

- 10.3 ☒ AND, any disclosure of personal information to another federal institution or outside the Government of Canada is governed by a formal agreement or arrangement (e.g., a Memorandum of Understanding, an accord, a contractual arrangement, etc.) to ensure that appropriate privacy protection clauses are included, and, where applicable, include provisions for inter-jurisdictional or transborder flows of personal information. Such clauses must cover the following topics:
- a) Control over personal information, where appropriate.
 - b) Limitations on the collection, retention, use and disclosure of personal information.
 - c) Measures (administrative, technical and physical) to protect the integrity and confidentiality of personal information.
 - d) Measures governing the disposition of the personal information, where relevant
 - e) Measures to ensure or verify that the personal information is only used for the purposes related to the agreement, arrangement or contract.
 - f) Obligations are to be extended to other parties such as subcontractors.

Details: The Mobile Device Management component is hosted at Rogers however a small group of security cleared employees may remotely access a device for support purposes. This access will be controlled by the user who will be prompted to allow remote access to a device. Users will be advised not to grant access while processing personal information which will effectively eliminate access to personal information.

NO

- 10.4 ☐ There is no disclosure of personal information within or outside the institution for purposes that are directly related to the administration of the program or activity.

11. Accounting for New Uses or Disclosures Not Reported in CBSA Info Source

Will controls and procedures be implemented to account for any new use or disclosure of the personal information that is not included in the relevant PIB published in CBSA Info Source?

YES

- 11.1 ☒ Appropriate controls and procedures have been or will be implemented to ensure that:
- a) the head of the institution (The ATI and Privacy Director) or the appropriate delegate is notified about any new use or disclosure of personal information that is not reflected in the PIB description published in *CBSA Info Source*;
 - b) the consent of the individual to whom the information relates is obtained in writing, as appropriate, prior to any new use of the information for an administrative purpose that is not reflected in the relevant PIB published in *CBSA Info Source*, unless the new use is considered to be consistent with the purpose for which the personal information was obtained or compiled and the Privacy Commissioner is notified, by the CBSA ATI and Privacy Director, forthwith regarding the new consistent use;
 - c) except as permitted under subsection 8(2) of the *Privacy Act*, any disclosure of personal information for a purpose that is not reflected in the relevant PIB published in *CBSA Info Source* will only be made with the consent of the individual to whom the information relates;
 - d) a record is kept for any new use or disclosure of personal information not described in the relevant PIB published in *CBSA Info Source*, and that this record is stored with the personal information to which it relates and retained for a minimum period of two years following such a use or disclosure;
 - e) if the information is disclosed to a federal investigative body under paragraph 8(2)(e) of the *Privacy Act*, the record of disclosure will be kept in a separate PIB for a period of two years where it will be available to the Privacy Commissioner for review upon request;
 - f) the Privacy Commissioner is notified, by the CBSA ATI and Privacy Director, forthwith, as required under subsection 9(4) of the Act, of any new use or disclosure that is consistent with the purpose for which the information was obtained or compiled, but which is not reflected in the relevant PIB published in *CBSA Info Source*;
 - g) the relevant PIB is amended in time for the next edition of *CBSA Info Source* to include any new use(s) or disclosure(s) that are consistent with the purpose for which the information was obtained or compiled, as well as any routine use(s) or disclosure(s) that do not fall within the categories of purpose of collection or consistent use; and
 - h) the Privacy Commissioner is notified, by the ATI and Privacy Director, prior to or forthwith, as required under subsection 8(5) of the Act, about any disclosures made or to be made in the public interest or in the interest of the individual to whom the information relates.
 - i) Other

NO

- 11.2 ☐ Please explain why such controls and procedures will not be implemented

Detail: Provide adequate justification.

12. Safeguards - Statement of Sensitivity

Has a Statement of Sensitivity (SoS) or similar analysis been completed to assess the degree of sensitivity of the personal information to be collected and retained for the program or activity?

YES

- 12.1 ☒ The information contained in the SoS or similar analysis has been taken into account when assessing the level of risks to privacy in "Section 2 - Risk Area Identification and Categorization" of the CBSA PIA.

Details: A Statement of Sensitivity has been prepared. The information collected by handhelds was identified as Protected B.

NO

- 12.2 ☐ Please explain why a SoS or similar analysis was not considered necessary to assess the sensitivity of the information.

13. Safeguards - Threat and Risk Assessment

Has a Threat and Risk Assessment (TRA) or a similar security assessment been completed for the program or activity? (Input to this section must be coordinated with and reviewed by CBSA – IT - Security Directorate)

YES

- 13.1 ☐ Reference the title of the TRA or other security assessment in "Section 6 – Supplementary Documents List" and provide a brief synopsis of the assessment in the space below:

Details :

- 13.2 ☐ AND, obtain assurances from the officials responsible for the program or activity that the measures recommended in the assessment have been implemented to ensure the confidentiality, availability and integrity of the personal information.
- 13.3 ☐ AND, ensure that any residual risks to personal information are known and accepted by the executive or senior official responsible for the program or activity and the Head or delegated authority for the Privacy Act. (ATI and Privacy Director)

NO

- 13.4 ☒ If a TRA or similar security assessment is underway, simply reference that fact in the space below and indicate when it is likely to be completed. If there is no intent to complete one, please explain.

Details: A Security review of the wireless handheld project is underway.

14. Safeguards - Administrative, Physical and Technical

Please identify below any administrative, physical and technical safeguards in place, or to be implemented, for this program or activity to ensure the confidentiality, availability and integrity of the personal information.

Please check all that apply, including safeguards identified by the TRA or similar security assessment.

14.1 Administrative safeguards

- ☒ Internal security and privacy policies and procedures
- ☒ Staff training on privacy and the protection of personal information
- ☒ Screening and security checks of employees
- ☒ Appropriate security levels for employees who will have access to personal information
- ☒ Contingency plans and documented procedures in place to identify and respond to security and privacy breaches, and to communicate security violations to the data subject, law enforcement authorities and relevant program managers
- ☒ Regular monitoring of users' security practices
- ☒ Methods to ensure that only authorized personnel who need to know have access to personal information
- ☒ Other

Details: All those with access will be reminded of security and privacy considerations as part of the information sessions being provided. Security screening and checks are carried out on a regular basis in accordance with standard CBSA protocol. Contingency plans for security violations have been documented. Users access to information is full audited and access to information is controlled based on assignment of roles which are granted on an as needs basis.

14.2 Physical safeguards

- ☒ Restricted access areas
- ☐ Security guards
- ☒ Identification badges are worn by staff at all times
- ☒ After hours alarms and monitoring systems
- ☐ Locked filing cabinets
- ☐ Combination locks
- ☒ Video surveillance (closed-circuit television)
- ☒ Secured server locations
- ☒ Backups secured off-site
- ☒ Other

Details: Personal information will rarely be stored on a device however: Wireless handhelds will be stored in areas that have restricted access and when in use they will be carried by a BSO. All BSOs are uniformed, any other staff on site are required to wear identification. After hour alarms and monitoring systems are in place at all POEs. Servers are located in secure rooms. Devices will be fitted with if found messaging to ensure that if they are lost they can be returned.

14.3 Technical safeguards

- ☒ Role-based user authorization and authentication
- ☒ Passwords (minimum of 6 characters long, include alpha and numeric characters)
- ☒ Passwords are changed by users every 90 days and recently used passwords cannot be re-used)
- ☒ Password protected screensavers
- ☒ Session-time out security (automatically locks an account after a session has been idle for a specified amount of time)
- ☒ Firewalls
- ☒ Virtual Private Network (VPN)
- ☒ Encryption of sensitive information
- ☒ Government of Canada Public Key Infrastructure Certificates (PKI)
- ☐ External Certificate Authority (CA)
- ☒ Audit trails
- ☒ Other

Details: Role based user authentication is required to access the application. In addition a pin is required to gain access to the application logon. Passwords are managed as per CBSA protocols. Users will be required to enter a password after 15 minutes of inactivity and a pin, user ID and password (6 characters with number) after 1 hour of inactivity – a device will be wiped after 11 failed attempts making the device unusable. Firewalls are in place. The current VPN offerings from CRA and SSC cannot be leveraged for the MOPI device. The CBSA has provisioned Net Motion Mobility Services for the VPN and encryption of data at rest and data in transit (whether via cellular or Wi-Fi). Currently we are using Pre-Shared Key (PSK) while Public Key Infrastructure (PKI) engineering continues. The PKI option is expected to be introduced shortly after the end of fiscal 2016/17. All data is audited. Mobile device management allows authorized users to limit device policy, monitor device usage and location and administer security measures such as a remote wipe or locking of a device in case of breaches in security.

15. Technology and Privacy - Tracking Technologies

Will the information system(s) used to deliver the program or activity employ cookies or other tracking technologies to collect personal information about users and their transactions?

YES

- 15.1 ☐ The specific tracking technologies to be used is adequately described under Part 6: Technology and Privacy of "Section 2 – Risk Area Identification and Categorization" of the CBSA PIA;
- 15.2 ☐ AND, the collection of any personal information using such technologies is reflected in the relevant **PIB** and in "Section 3 – Analysis of Personal Information Elements" of the CBSA PIA;
- 15.3 ☐ AND, the use of such technologies to collect information about users and their transactions is adequately reflected in the "**Privacy Notice**";
- 15.4 ☐ AND, those responsible for implementing and using tracking technologies to collect personal information or who may have access to personal information collected through these methods are made aware of privacy and security policy requirements;
- 15.5 ☐ AND, where personal information collected through such tracking technologies is used to make a decision that directly affects the individual to whom the information relates, it will be retained for a

minimum of two years after the last administrative action as required under the *Privacy Regulations*.

NO

15.6 ☒ Tracking technologies are not used to collect personal information about users.

16. Technology and Privacy - Surveillance or Monitoring

Will the new or modified program or activity result in new or increased surveillance or monitoring of a targeted population?

YES

- 16.1 ☐ Consult with your legal advisors to determine whether or not such surveillance or monitoring activities raise any issues relating to the *Charter of Rights and Freedoms*, the *Privacy Act* or other applicable acts.
- 16.2 ☐ And, ensure the surveillance or monitoring method(s) to be used, the characteristic(s) of the targeted population and the scope of the surveillance or monitoring are adequately described under Part 6: Technology and Privacy of "*Section 2 – Risk Area Identification and Categorization*" of the CBSA PIA.
- 16.3 ☐ AND, any personal information collected or created as a result of such surveillance or monitoring is described in the relevant **PIB** and in *Section 3 – Analysis of Personal Information Elements* of the CBSA PIA.
- 16.4 ☐ AND, the collection or use of personal information through surveillance or monitoring is adequately reflected in the "**Privacy Notice**", unless such notification might result in the collection of inaccurate information or defeat the purpose or prejudice the use for which the personal information is collected.
- ☐ If notice about surveillance or monitoring will not be provided

Detail explain why:

- 16.5 ☐ AND, those responsible for implementing and using such surveillance or monitoring method(s) or who may have access to personal information collected or created through these methods are made aware of privacy and security policy requirements.

NO

16.6 ☒ The new or modified program or activity will not result in additional surveillance or monitoring.

17. Considerations Related to Compliance, Regulatory Investigation, Enforcement

Does the program or activity involve compliance/regulatory investigation or law enforcement, surveillance or intelligence gathering that targets specific individuals against whom penalties, criminal charges or sanctions may be applicable?

YES

- 17.1 ☒ Consult with your legal advisors to determine whether or not the compliance/regulatory investigation or law enforcement activities raise any issues relating to the *Charter of Rights and Freedoms*, the *Privacy Act* or other applicable acts.
- 17.2 ☒ AND, identify the legislative authority and the specific regulatory or law enforcement purpose involved:

Details: Legal authority for the collection of personal information via traveller processing is derived from multiple, inter-related legislations and regulations.

o Information required from individuals as they request entry into Canada is derived from two legislations. 1) Section 11 of the *Customs Act*, which states, "every person arriving in Canada shall, except in such circumstances and subject to such conditions as may be prescribed, enter Canada only at a customs office designated for that purpose that is open for business and without delay present himself or herself to an officer and answer truthfully any questions asked by the officer in the performance of his or her duties under this or any other Act of Parliament." And 2) Section 18(1) of the *Immigration and Refugee Protection Act* which states, "Every person seeking to enter Canada must appear for an examination to determine whether that person has a right to enter Canada or is or may become authorized to enter and remain in Canada."

In addition to these specific legal authorities, information is also collected under the *Proceeds of Program legislation* as defined in the *Canada Border Services Act* "means any other Act of Parliament or any instrument made under it, or any part of such an Act or instrument,

(a) that the Governor in Council or Parliament authorizes the Minister, the Agency, the President or an employee of the Agency to administer and enforce, including the *Customs Act*, the *Customs Tariff*, the *Excise Act*, the *Excise Act, 2001*, the *Immigration and Refugee Protection Act* and the *Special Import Measures Act*;

(b) that the Governor in Council or Parliament authorizes the Minister, the Agency, the President or an employee of the Agency to enforce, including the *Agriculture and Agri-Food Administrative Monetary Penalties Act*, the *Canada Agricultural Products Act*, the *Feeds Act*, the *Fertilizers Act*, the *Fish Inspection Act*, the *Health of Animals Act*, the *Meat Inspection Act*, the *Plant Protection Act* and the *Seeds Act*;

(c) under which the Minister or another minister authorizes the Agency, the President or an employee of the Agency to administer a program or carry out an activity; or

(d) under which duties or taxes collected and paid pursuant to the *Customs Act* are imposed."

- 17.3 ☐ AND, if the legislative authority differs from the legal authority for the program or activity, ensure it is adequately reflected in the response to Question 1 of "Section 5 – Privacy Compliance Analysis" and in "Section 1 – Overview and PIA Initiation" of the CBSA PIA.
- 17.4 ☐ AND, any personal information collected or created as a result of such regulatory or criminal enforcement, surveillance or intelligence gathering program or activity is described in the relevant **PIB** and in "Section 3 – Analysis of Personal Information Elements" of the CBSA PIA.

- 17.5 ☐ AND, the collection or use of personal information through these compliance / regulatory investigation or enforcement activities is adequately reflected in the "**Privacy Notice**", unless such notification might result in the collection of inaccurate information or defeat the purpose, or prejudice the use, for which the personal information is collected.

Details:

- ☐ If notice about the compliance/regulatory investigation or law enforcement activities will not be provided.

NO

- 17.6 ☐ The program or activity does not involve the conduct of regulatory or criminal enforcement, surveillance or intelligence gathering.

SECTION 6 - Summary of Analysis and Recommendations

(L)ow: There is a remote possibility that the risk will materialize and/or the impact of the risk to the program is minor.

(M)oderate: The possibility of the risk materializing is very low although the impact of such a risk is high, *OR* the possibility of the risk materializing is high but the impact of such a risk is minor, *OR* the impact and likelihood of the risk occurring are both determined to be moderate.

(H)igh: There is a near certainty that the risk will materialize if no corrective measures are taken and/or the impact of the risk on the program is severe.

Necessity to Collect Personal Information

No risks identified.

Authority for the Collection, Use or Disclosure of the Social Insurance Number

No risks identified.

Direct Collection - Notification and Consent

- 1) Signage notifying all travellers that their information will be collected is not in place at all ports of entry.

Mitigation: Given information collection at our POEs is an ongoing activity this risk requires resolution at a level much larger than the Wireless Handheld project.

Risk Rating: Minor

Indirect Collection - Consent or Authority under Sec. 10 of Privacy Regulations

No risks identified.

Indirect Collection - Without Notification and Consent

No risk identified.

Retention and Disposal of Personal Information

- 1) CBSA retention period for data collected via traveller processing in this case is 7 years.

Mitigation: CBSA to conduct a review of the retention period for information collected via traveller processing, and explore the possibility of aligning the traveller processing records for entry, which are currently retained for seven years, with the retention period for Entry/Exit initiative (exit records), which is set for 15 years retention past the point of collection.

Risk Rating: Minor

Accuracy of Personal Information

No risks identified

Use of Personal Information

- 1) Concerns could be raised regarding the use of data collected.

Mitigation: All data collected is used in accordance with established parameters. Data collected is collected under the legal terms of the Customs Act.

Risk Rating: Minor

Disclosures Directly Related to the Administration of the Program or Activity

No risks identified.

Accounting for New Uses or Disclosures Not Reported in CBSA Info Source

No risks identified.

Safeguards

- 1) **IPIL access is available at most sites where the handheld devices will be deployed. Using the handheld device rather than IPIL increases the risk to the personal information of travellers.**

Mitigation: At these sites handhelds represent an essential tool to allow officers to stay with travellers, thereby increasing security and control of the situation for both travellers and officers. The risk to the security and control of the situation outweigh the risks to the information of travellers.

Risk Rating: Minor

- 2) **CBSA project processes stipulate Security Assessment Report (SAR) as the approved Agency project document instead of a Threat and Risk Assessment (TRA). The Security Assessment Report is underway.**

Mitigation: The SAR is underway – resourcing issues may impede its completion.

Risk Rating: High

- 3) **Devices could be misplaced or stolen.**

Mitigation: While a device may be misplaced or stolen several items limit the risk associated to this loss:

- a. In 99% of circumstances there is no information stored on the device.
- b. Any information on the device will be encrypted (info on device only in rare circumstances).
- c. Device access is restricted with a PIN and/or user ID and password.
- d. Devices will wipe with 11 failed password attempts.
- e. Device can be located, locked and wiped remotely.
- f. Device will have 'if found' messaging and contact information to facilitate safe return.

Risk Rating: Minor

- 4) **Interception of Wireless Transmission.**

Mitigation: Data in wireless transit via Wi-Fi or cellular will be encrypted thereby limiting risk. In addition there is intrusion detection system. This means that should a non-authorized user try to connect to the network it will be detected and shut down the connection.

Risk Rating: Moderate

- 5) **Loss of Connectivity**

Mitigation: If connectivity is lost, it is possible in very rare circumstances that a device will have personal information on it. Connectivity is expected to be stable. All information would be encrypted.

Risk Rating: Minor

6) Cellular connections could roam to U.S. towers at some locations.

Mitigation: This will be mitigated by eliminating the capacity for device signal to roam.

Risk Rating: Minor

7) Remote viewing by third party vendor for support via MDM.

Mitigation: This will be mitigated by requiring notification and acceptance of the request for access by the user prior to the vendor remotely accessing a device. BSOs will be briefed to ensure that when remote access is granted to a third party vendor for support that no personal information is available on the device. In addition, all those with access will be security cleared to enhanced reliability.

Risk Rating: Moderate

Technology and Privacy - Tracking Technologies

No risks identified.

Technology and Privacy - Surveillance or Monitoring

1) A camera is part of the device and could be perceived to be used for surveillance or monitoring.

Mitigation: The camera will be disabled and will not be available for use.

Risk Rating: Minor

Considerations Related to Compliance, Regulatory Investigation, Enforcement

No risks identified.

SECTION 7 - SUPPLEMENTARY DOCUMENTS LIST

Documents used or related to the CBSA PIA may include:

- Info Source, Canada Border Services Agency Chapter
- Privacy Impact Assessment, PIK, December 2016
- Custom Act
- Architecture and Design Specification (ADS) Part 1
- Architecture and Design Specification (ADS) Part 2
- Architecture and Design Specification (ADS) Part 3
- Architecture and Design Specification (ADS) Part 4

SECTION 8 - FORMAL APPROVAL

The following signature represents a commitment to comply with sections 4 to 8 of the *Privacy Act* and the related privacy policy requirements outlined in the CBSA PIA as they relate to the administration of the identified program or activity.



 Martin Bolduc, Vice President, Programs Branch

JUN 02 2017

Date

Note: Responsibility for sections 4 to 8 of the *Privacy Act* rests with all employees of government institutions that handle personal information. Officials who manage such programs and activities are responsible for ensuring that such requirements are implemented as part of the administration of the program or activity.

The following signature represents a commitment by the Head of the institution or his/her delegate(s) who is responsible for establishing personal information banks in accordance with section 10 of the *Privacy Act*.


 Dan Proulx, Director, Access to Information and Privacy Division

MAY 31 2017

Date

Note: Under the *Privacy Act*, the Head or his/her delegate(s) is responsible for complying with legal and relevant privacy policy requirements related to the approval and registration of personal information banks

Annex A: Privacy Compliance Checklist and Other Considerations

Privacy Compliance Analysis question #	Action required to support legal and policy compliance (cross reference to relevant question of <i>Section 5 – Privacy Compliance Analysis</i>)	Done	To be done
1	Legal authority for the program or activity has been established and is reflected in the relevant PIB.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2	a) The categories and elements of personal information to be collected for the new program or activity have been carefully assessed based, for example, on the CBSA's experience gained with the administration of a similar program or activity. The personal data collected will be limited to only that which is required.)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	b) Categories and elements of personal information have been described in the relevant PIB for the program or activity.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	c) Controls and procedures will be implemented to ensure the CBSA does not collect more personal information than necessary for the program or activity and that a continuing need exists for the personal information and its collection.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
4 and 5	a) All of the requisite "Privacy Notices" and "Consent Statements" that meet the requirements of sections 6.2.9 to 6.2.12 of the <i>Directive on Privacy Practices</i> have been drafted. (Texts of the notices and consent statements must be included as an annex.)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	b) Controls and procedures have been implemented to keep records of individual consents, and to ensure that persons acting on behalf of individuals who do not have the capacity to provide consent have the authority to do so under section 10 of the <i>Privacy Regulations</i> .	<input checked="" type="checkbox"/>	<input type="checkbox"/>
7	a) A Records Disposal Authority (RDA) has been approved by Library and Archives Canada to authorize the disposal of the records containing personal information for the program.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	b) Controls and procedures have been implemented within the program or activity and the CBSA ATI and Privacy Division to ensure that information that has been used for an administrative purpose will be kept for the minimum retention period established by the Privacy Regulations.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	c) Reference to the RDA, the retention period and the disposition standards for the program have been cited in the relevant PIB.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
8	Controls and procedures are in the process of being implemented to ensure that the personal information associated with the program is as accurate, complete and up-to-date as necessary.	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Privacy Compliance Analysis question #	Action required to support legal and policy compliance (cross reference to relevant question of <i>Section 5 – Privacy Compliance Analysis</i>)	Done	To be done
---	---	------	---------------

**Other Privacy Considerations related to specific principles that are not explored in the previous 17 sections:
(these considerations should be explored in the Executive Summary)**

Openness	Describe how the results of any privacy impact assessment or audit will be made available to the public. The Executive Summary will be published on the external CBSA ATI and Privacy Division website at http://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/pia-efvp/atip-aiprp/pias-sefp-eng.html	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Are policies and practices relating to the proposal's management and handling of personal information available to the public?	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Is there a communications plan to explain to the public how personal information will be managed and protected?	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Is there a clearly defined and easy process for individuals to access such information and/or communicate with appropriate individuals with respect to policies and practices relating to management and protection of personal information?	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Where appropriate, will public consultation take place on the privacy implications of the proposal?	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Individual's Access to Personal Information	Is the system designed to ensure that an individual can have access to his/her personal information, including all other programs or applications that have received copies of the information? s. 12(1)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Are there documented procedures developed or planned on how to make privacy requests or requests for the correction of personal information? s. 12 (2)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Are individuals provided with access to their personal information in the official language of their choice? s. 17(2)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	If appropriate, are individuals provided with access to their personal information in an alternative format? s. 17(3)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Challenging Compliance	Are the complaint procedures for the proposed program or service consistent with legislated requirements? s. 29-35	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	To improve information management practices and standards, has a procedure been established to log and periodically review the nature, frequency and resolution of complaints?	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Entry/Exit Wireless Handhelds

PIA

Privacy Compliance Analysis question #	Action required to support legal and policy compliance (cross reference to relevant question of <i>Section 5 – Privacy Compliance Analysis</i>)	Done	To be done
	Are there oversight and review mechanisms implemented or available to ensure accountability?	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Have oversight agencies, including the Office of the Privacy Commissioner, issued reports or opinions on issues that would be relevant to the proposal?	<input checked="" type="checkbox"/>	<input type="checkbox"/>

CBSA
PROTECTION • SERVICE • INTEGRITY

ASFC
PROTECTION • SERVICE • INTÉGRITÉ

Application for Declaration of Relief Under Subsection 42.1(1) of the IRPA

Privacy Impact Assessment (PIA)

Immigration Enforcement Policy Unit
Enforcement and Intelligence Programs, Programs Branch
March 2017

Canada

Name of Program / Activity / Service

PIA

Version Control

Version	Author	Action	Date
1.0	Lyne Pelletier	Creation of document includes Treasury Board Secretariat policy requirements (2010). Incorporates more detailed privacy analysis to reflect expectations of the Office of the Privacy Commissioner (2011). User friendly with examples and explanatory notes. Includes an Action Plan for implementing mitigating strategies.	March 15, 2012
1.0	Dan Proulx	Approved ver. 1.0	March 28, 2012
1.1	Lyne Pelletier	Oak Test and Privacy Principles added to template	November 07, 2012
1.2	Dan Proulx	Approved ver. 1.1	November 15, 2012

Change Control Table

Version	Date	Change Made By	Change Requested By	Change
2	21/9/2015	R. Gilbert	J. Robertson	Format, misc.
3	22/10/2015	R. Gilbert	J. Robertson / A. Courtemanche	Incorporated suggested changes
4	10/2/2016	R. Gilbert	R. Gilbert	Additional revisions all parts
5	15/04/2016	R. Gilbert	G. Calma	Operational area revisions
6	17/05/2016	R. Gilbert	G. Calma / J. Robertson	Edits/revisions
7	24/5/2016	R. Gilbert	G. Calma / T. Vansickle	Edits/revisions
8	31/08/2016	P. Lopez	Adam Norwick	Edits/revisions
9	28/10/2016	P. Lopez	Neil O'Brien	Re-write into proper template
10	16/12/2016	G. Calma / J. Campbell	Martin Leroux	Edits/revisions
11	26/01/2017	G. Calma	G. Calma / T. Vansickle	Edits/revisions
12	02/02/2017 07/02/2017 09/02/2017	G. Calma	G. Calma / T. Vansickle	Final edits/ revisions
13	20/02/2017	J. Robertson	R. St. Marseille	To integrate comments from DO

Table of Contents

VERSION CONTROL	2
EXECUTIVE SUMMARY.....	6
ABBREVIATIONS AND ACRONYMS	9
DEFINITIONS.....	11
SECTION 1 - OVERVIEW AND INITIATION	14
SECTION 2 - RISK AREA IDENTIFICATION AND CATEGORIZATION	20
Type of Program or Activity	20
Type of Personal Information Involved and Context.....	22
Program or Activity Partners and Private Sector Involvement.....	22
Duration of the Program or Activity	23
Program Population	23
Technology and Privacy	23
Personal Information Transmission	24
Risk Impact to the CBSA.....	25
Risk Impact to the Individual or Employee	25
SECTION 3 - ANALYSIS OF PERSONAL INFORMATION ELEMENTS	26
SECTION 4 - FLOW OF PERSONAL INFORMATION	38
1. Applicants use form BSF 766E, available in PDF format from the CBSA website. They may complete and submit the form and any supporting documentation, in paper, electronic or both formats.	38
4.2 Data Flow Model - Table	40
4.3 Internal Use and Disclosure	41
4.4 External Use and Disclosure.....	41
4.5 Retention / Storage.....	44
4.6 Other Possible Considerations.....	44
SECTION 5 - PRIVACY COMPLIANCE ANALYSIS	46
1. Legal Authority For Collection Of Personal Information (if unsure, consult with Legal Services)	46
2. Necessity To Collect Personal Information	47
3. Authority For the Collection, Use or Disclosure Of the Social Insurance Number... ..	47
4. Direct Collection - Notification and Consent (as appropriate)	48
5. Indirect Collection - Consent or Authority Under Sec. 10 of Privacy Regulations....	50
6. Indirect Collection - Without Notification and Consent	50
7. Retention and Disposal of Personal Information.....	51
8. Accuracy Of Personal Information	53
9. Use Of Personal Information	54
10. Disclosures Directly Related to the Administration of the Program or Activity.....	55
11. Accounting For New Uses or Disclosures Not Reported in CBSA Info Source	58
12. Safeguards - Statement Of Sensitivity	59
13. Safeguards - Threat and Risk Assessment	60
14. Safeguards - Administrative, Physical and Technical.....	60
15. Technology and Privacy - Tracking Technologies	62

16. Technology and Privacy - Surveillance or Monitoring	63
17. Considerations Related to Compliance, Regulatory Investigation, Enforcement ..	64
SECTION 6 - SUMMARY OF ANALYSIS AND RECOMMENDATIONS.....	66
SECTION 7 - SUPPLEMENTARY DOCUMENTS LIST	68
SECTION 8 - FORMAL APPROVAL	69
ANNEX A: PRIVACY COMPLIANCE CHECKLIST AND OTHER CONSIDERATIONS.....	70
ANNEX B: OFFICE OF THE PRIVACY COMMISSIONER EXPECTATIONS	73
ANNEX C: CATEGORIES OF PERSONAL INFORMATION	76

Privacy Impact Assessment Date / Version:	2017-03-10
Office of the Privacy Commissioner file #:	
Project Implementation Plan (if applicable)	
Federal Institution:	Canada Border Services Agency (CBSA)
Related Class of Record Number:	CBSA ENF 130
Personal Information Bank:	CBSA PPU 1504
Government Official Responsible for PIA:	Vice President, Programs Branch
Delegate for section 10 of the <i>Privacy Act</i> :	ATI and Privacy Director

EXECUTIVE SUMMARY

This Privacy Impact Assessment (PIA) examines privacy risks associated with the CBSA's Ministerial Relief program and planned regulatory amendments for Ministerial relief, including the requirement that applicants complete a standardized application form.

Under existing legislation, foreign nationals who are believed to be or found to be inadmissible to Canada under the *Immigration and Refugee Protection Act* (IRPA) on the basis of security, certain provisions relating to human or international rights violations, or organized criminality may seek a declaration of relief from the Minister of Public Safety and Emergency Preparedness (Minister) under subsection 42.1(1) of the IRPA. If the Minister decides to make a declaration of relief, the original grounds for inadmissibility no longer apply. The foreign nationals may then pursue temporary or permanent resident status without their applications being rejected because of the same grounds of inadmissibility for which relief was granted. It is important to note that the Ministerial relief process and the admissibility process are two separate processes and this PIA only addresses Ministerial relief. The collection of data from the admissibility process is not impacted.

There is currently no formalized application framework for Ministerial relief. Foreign nationals typically request relief by providing documentary submissions with varying degrees of relevance to a decision on whether or not to grant relief. Currently, there are also no formal criteria establishing when a person may apply for relief. Until recently, Immigration, Refugees and Citizenship Canada officers were directed to refer a person for consideration for Ministerial relief and to await the outcome of the relief process prior to either rejecting their immigration application (i.e., temporary or permanent resident application) or referring allegations of inadmissibility to the Immigration and Refugee Board (IRB) for determination. As a result, the current Ministerial relief inventory includes applications from individuals who have yet to receive a final decision on admissibility. This has resulted in resources being used to assess applications of individuals who may not be inadmissible, and as a result, may not require Ministerial relief. Amendments to the *Immigration and Refugee Protection Regulations* (IRPR) are designed to bring greater clarity, consistency and control to the Ministerial relief application process, case intake and inventory management. These amendments will:

- establish when a foreign national may submit an application (e.g., once a final inadmissibility determination has been made, including exhausting all legal challenges). This will allow the CBSA to focus resources on processing Ministerial relief cases where inadmissibility has already been established and upheld by the IRB or courts, and will effectively reduce the future intake of cases where MR is not required;
- require applicants to use the prescribed application form;

- allow the CBSA to return an application, unprocessed, when certain requirements are not met;
- allow applications to be closed when an applicant does not respond to a notice requiring them to confirm their intention to proceed with their application within the specified timeframe, or when other remedies have been obtained;
- require applicants to provide the Minister with updated address and contact information while applications for Ministerial relief are in process; and
- address transitional cases (cases already in progress at the time the new framework is implemented) impacted by the new regulations by clarifying which aspects of the proposed regulatory amendments would apply to those requests for Ministerial relief received prior to the coming-into-force of these proposed regulatory amendments.

The proposed regulatory amendments were pre-published in the *Canada Gazette* in June 2015. Final publication is expected upon the regulations coming into force, after which use of the application form will be required for all new applicants for Ministerial relief.

Legislative Authority

Authority for this collection, use and disclosure of personal information is found in the *IRPA* (sections 15.1, 16.1, 34, 35(1)(b), 37(1), 42.1), and the amended *IRPR* (sections 24.1-5).

Scope

This PIA assesses the management of personal information collected, used, disclosed and retained by the CBSA during the MR application process only.

Necessary, Effective, Proportionate and Minimal

The personal information collected, used, disclosed and retained under this initiative is necessary to support the Agency's research and advice to the Minister of Public Safety on the merits of an application for Ministerial relief. The proposed measures will augment the effectiveness of the MR application process by requiring the timely provision of information relevant to the assessment process. Collection and disclosure is minimized to safeguard the rights of applicants, and to reduce the risk of a breach of their personal information. The information collected under this initiative will be used to inform advice and recommendations to the Minister. By prescribing a defined process, the use of an application form, limiting the time during which files remain open, and applying a record disposition schedule, the CBSA believes the Ministerial relief process impairs as little as possible the privacy rights of the applicants.

Protecting your Personal Information

The following personal information elements will be managed by the CBSA Ministerial Relief Unit (MRU):

- The applicant's place of birth, gender, marital status, and the names of any former spouses or common-law partners;
- The applicant's telephone number and email address, if any;
- The applicant's former countries of citizenship or former countries of nationality;
- The applicant's education, including the name and location of all elementary and secondary schools and post-secondary, technical and vocational institutions attended and the start and end dates for the periods during which they attended each school or institution;
- The applicant's work history, including volunteer work, beginning from the age of 16 years, including

start and end dates for each period of work, their job title and work description and the employer's name and address;

- The applicant's international travel history beginning from the age of 16 years, including a list of the countries visited, the purpose of the visits, the dates and duration of the visits and any immigration status sought from or granted by any country visited; and
- Whether the applicant was determined to be inadmissible under section 34, paragraph 35(1)(b) or (c) or subsection 37(1) of the IRPA, the date on which and the city and country in which the determination was made and whether the determination resulted in a decision referred to in paragraph 24.1(1)(a) or a removal order referred to in paragraph 24.1(1)(b).

The above-listed information will be collected via a standardised application form BSF 766E (see attached) created by the CBSA, to be completed by the applicant and delivered to the MRU accompanied by any additional information the applicant feels relevant to the national interest assessment.

This information will be assessed, along with information related to the applicant and the activity in which they participated or groups of which the applicant was a member that is in the control of the CBSA from the former Field Operations Support System (FOSS), the National Case Management System (NCMS), the Global Case Management System (GCMS), the Secure Tracking System (STS), Computer-Assisted Immigration Processing System (CAIPS), Case Processing System (CPS), as well as any information from the Canadian Police Information Centre (CPIC) that might be relevant. This information is assessed by analysts of the MRU and they will provide a recommendation and reasons to the Minister for a final decision on individual applications. The recommendation, as well as the information used in support of the recommendation, is disclosed to the applicant; any sensitive information provided by partner agencies will be redacted prior to disclosure to the applicant.

Right of Access

A privacy notification statement will appear on the application form explaining the reason this information is being collected, how the information will be used, to whom it may be disclosed and how the applicant may make a complaint. When the CBSA has prepared a recommendation for the Minister, a copy of the recommendation, and all information used in support of the recommendation (less any third party information that has been redacted), is provided to the applicant. The applicant is invited to make any additional submissions prior to the recommendation and associated documents being referred to the Minister for decision. Personal information collected will be retained for a period of 80 years or when the individual is 100 years of age and only after the file has been closed.

Applicants may formally request access to their personal information, or access to corporate records related to or created by the MRU by contacting the Access to Information and Privacy Division. More information about this can be found at: <http://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/pia-efvp/atip-aiprp/menu-eng.html>.

Accountability

Applicants with concerns about the collection, use, disclosure or retention of their personal information may issue a complaint to CBSA Access to Information and Privacy Division. Complaints should be made in writing, and include the applicant's name, contact information, and a brief description of the concerns. Contact information for the Access to Information and Privacy Division at the CBSA can be found at: <http://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/pia-efvp/atip-aiprp/contact-eng.html>.

ABBREVIATIONS AND ACRONYMS

Note: Using the table format below, list any abbreviations and acronyms that are used in this report. Expand the list to include acronyms specific to the program or initiative, as necessary.

The following is a list of abbreviations and acronyms used in this report:

ATIP	Access to Information and Privacy
APR	Application for Permanent Residence
BBH	BlackBerry Hand Held Device (smart phone)
BBS	BlackBerry Service
CBSA	Canada Border Services Agency
CAIPS	Computer-Assisted Immigration Processing System
CLF	Common Look and Feel
COR	Class of Record
CPIC	Canadian Police Information Centre
CSE	Communications Security Establishment
CSIS	Canadian Security Intelligence Service
DOJ	Department of Justice
DSO	Departmental Security Officer
FOSS	Field Operations Support System
GCMS	Global Case Management System
GOC	Government of Canada
GSP	Government of Canada Security Policy
HQ	Headquarters
ID	Identification
INTERPOL	International Criminal Police Organization
IRB	Immigration and Refugee Board
IRCC	Immigration, Refugees and Citizenship Canada (formerly Citizenship and Immigration Canada)
IRPA	<i>Immigration and Refugee Protection Act</i>
IRPR	<i>Immigration and Refugee Protection Regulations</i>
ISA	Information Sharing Agreement
IT/IM	Information Technology/Information Management
LAN	Local Area Network

Name of Program / Activity / Service

PIA

MOU	Memorandum of Understanding
MR	Ministerial Relief
MRU	Ministerial Relief Unit
NCMS	National Case Management System
NCIC	National Crime Information Centre – an FBI database
OPC	Office of the Privacy Commissioner of Canada
PA	<i>Privacy Act</i>
PDF	Portable Document Format
PI	Personal Information
PIA	Privacy Impact Assessment
PIB	Personal Information Bank
RCMP	Royal Canadian Mounted Police
SOS	Statement of Sensitivity
SSC	Shared Services Canada
STS	Secure Tracking System
TBS	Treasury Board Secretariat
TRA	Threat and Risk Assessment
TRV	Temporary Resident Visa
VP	Vice-President
VPN	Virtual Private Network

DEFINITIONS

Note: Using the table format below, provide definitions of the terms frequently used in this report.

This section provides definitions of the terms frequently used in this report:

Action Plan	The Action Plan describes the steps that the Program will take to address risks that have been identified by ATI and Privacy Division, OPC and TBS.
Admissible	An admissible person is a person who has been determined to meet the criteria of the IRPA and the IRPR, and been determined not to be described by any of the grounds of inadmissibility described in the IRPA.
Administrative purpose	The <i>Privacy Act</i> defines an “administrative purpose” to be the use of an individual’s personal information in a decision-making process that directly affects that individual.
Confidentiality	The Government Security Policy (2002) defines “confidentiality” to be the attribute that information must not be disclosed to unauthorized individuals, because of the resulting injury to national or other interests, with reference to specific provisions of the <i>Access to Information Act</i> and the <i>Privacy Act</i> .
Consistent use	Is a use that has a reasonable and direct connection to the original purpose(s) for which the information was obtained or compiled. This means that the original purpose and the proposed purpose are so closely related that the individual would expect that the information would be used for the consistent purpose, even if the use is not spelled out.
Data Matching	A comparison of personal data obtained from a variety of sources, including personal information banks, for the purpose of making decisions about the individuals to whom the data pertains. Data matching is a specialized activity involving the collection, use and disclosure of personal information that is subject to the various requirements of the <i>Privacy Act</i> .
Foreign National	A foreign national is a person who is neither a Canadian citizen, nor a permanent resident, and includes a stateless person.
Inadmissible	The IRPA establishes specific criteria by which a person may be refused admission to Canada, or if already in Canada, may be subject to removal. An inadmissible person may not be granted temporary or permanent resident status in Canada, unless the IRPA allows for a specific remedy or exemption from the grounds of inadmissibility. In dealings with persons who may be inadmissible to Canada, officers control the admission and/or allow for the presence of persons in Canada by referencing the various inadmissibility provisions of the IRPA. Part 1, Division 4 of the Act makes distinctions based on categories of inadmissibility related to: <ul style="list-style-type: none"> • criminality; • organized criminality; • security; • human or international rights violations; • health; • financial reasons; • misrepresentation;

Name of Program / Activity / Service	PIA
	<ul style="list-style-type: none"> • non-compliance; • inadmissible family members. <p>A person may also inadmissible to Canada if they do not meet the criteria of the status for which they have submitted an application (ie a work permit, a study permit, or a class of permanent resident).</p>
Info Source	<p>Is a series of annual Treasury Board Secretariat publications in which government institutions are required to describe their institutions, program responsibilities and information holdings, including PIBs and classes of personal information. The descriptions are to contain sufficient clarity and detail to facilitate the exercise of the right of access under the <i>Privacy Act</i>. Data-matching activities, use of the SIN and all activities for which privacy impact assessments were conducted have to be cited in <i>Info Source</i> PIBs, as applicable. The <i>Info Source</i> publications also provide contact information for government institutions as well as summaries of court cases and statistics on access requests.</p>
Minister's Delegate	<p>The <i>Immigration and Refugee Protection Act</i> (IRPA) authorizes the Minister of Public Safety and Emergency Preparedness (PSEP) to delegate certain decision-making authorities to a Minister's delegate. In the context of an A44(2) review, a Minister's delegate has been delegated the authority to determine whether an inadmissibility report regarding a permanent resident or foreign national is well founded and may refer the report to the Immigration Division for an admissibility hearing, or, where the inadmissibility allegations fall within the jurisdiction of the Minister's delegate, issue the appropriate removal order.</p> <p>Inadmissibility allegations for reasons of security, violations of human or international rights, and organized crime fall solely under the jurisdiction of the delegated officials of the CBSA, and the delegated authority to review those inadmissibility reports can only be exercised by CBSA officials at the level of supervisor or above. Jurisdiction for other grounds of inadmissibility have been delegated by the Minister of PSEP to officials of both the CBSA as well as the Department of Immigration, Refugees and Citizenship Canada.</p> <p>Ministerial relief is one of the four non-delegable authorities listed under subsection 6(3) of the IRPA.</p>
Ministerial relief	<p>Under IRPA section 42.1, the Minister of Public Safety and Emergency Preparedness may grant relief to foreign nationals inadmissible to Canada on the basis of security, certain provisions relating to human or international rights violations, or organized criminality, if he is satisfied that it is not contrary to the national interest. This process is commonly referred to as Ministerial relief (MR).</p>
National Interest	<p>National interest is a broad, discretionary test applied by the Minister of Public Safety and Emergency Preparedness.</p>
Permanent Resident	<p>A person who has acquired permanent resident status and not subsequently lost that status under section 46 of the IRPA. A permanent resident has a qualified right to enter, remain, work, and study in Canada.</p>

Personal Information	Personal Information: Information about an identifiable individual as defined in section 3 of the <i>Privacy Act</i> . This definition, although lengthy, is not exhaustive, as indicated by the introductory phrase, "including, without restricting the generality of the foregoing". Information that is not specifically mentioned in the list may still be included in the definition of personal information if it qualifies as "information about an identifiable individual".
Personal Information Bank	Is a description of personal information that is organized and retrievable by a person's name or by an identifying number, symbol or other particular assigned only to that person. The personal information described in the personal information bank has been used, is being used, or is available for an administrative purpose and is under the control of a government institution.
Privacy	The Office of the Privacy Commissioner of Canada describes "privacy" as "... the right to control access to one's person and information about one's self. The right to privacy means that individuals get to decide what and how much information to give up, to whom it is given, and for what uses."
Secure Tracking System	The Secure Tracking System (STS) contains information on individuals involved in and/or associated with any organization involved in war crimes, crimes against humanity and/or terrorist activities, organized crime, money laundering, terrorist financing, people smuggling, or persons associated with criminal organizations, and whose admission or presence in Canada may be contrary to immigration or citizenship legislation. The primary role of STS is to screen Temporary and Permanent Resident (TR/PR) visa applications.
Temporary Resident	A temporary resident is a foreign national who has been authorized to enter Canada for temporary purposes under the IRPA.

SECTION 1 - OVERVIEW AND INITIATION

Report Objectives

This report is a Privacy Impact Assessment (PIA) for applications for Ministerial relief, processed by the Canada Border Services Agency (CBSA). The objectives of this PIA are:

- to review the business processes in order to identify the data flow of personal information;
- to analyze the collection, use, disclosure and retention of personal information;
- to determine if there are privacy risks associated with applications for Ministerial relief; and
- to provide recommendations on the mitigation or elimination of the risks.

The information presented in this report follows the Treasury Board of Canada Secretariat Privacy Impact Assessment policy and guidelines.

The purpose of a PIA process is to ensure that privacy is considered throughout the project development cycle. The results of a PIA are a documented guarantee that privacy issues have been identified and adequately addressed.

Government Institution: Canada Border Services Agency, Enforcement and Intelligence Programs

Government Official Responsible for the Privacy
Impact Assessment

Dan Proulx

Martin Bolduc, Vice-President, Programs Branch,
CBSA

CBSA ATI and Privacy Director

Name of Program or Activity of the Government Institution:

Application for Declaration of Relief under Subsection 42.1(1) of the IRPA

Description of Program or Activity:

The Ministerial Relief initiative falls under sub-program 5.1 Immigration Investigations in the CBSA's 2016-2017 Program Alignment Architecture. The Immigration Investigations Program investigates, reports, and arrests foreign nationals and permanent residents already in Canada who are, or may be, inadmissible to Canada as defined by the Immigration and Refugee Protection Act. Depending on the type of inadmissibility and the status of the person in question, inadmissibility reports are reviewed by either a Minister's Delegate or the IRB. When a person fails to appear for an immigration proceeding such as an examination, admissibility hearing or removal interview, a warrant for their arrest may be issued. Warrants may also be issued against a foreign national or permanent resident where a CBSA inland enforcement officer has reasonable grounds to believe that they are inadmissible to Canada.

Name of Program / Activity / Service

PIA

Description of the class of records associated with the program or activity:

Describes records related to investigations into Foreign Nationals (FN) or Permanent Residents (PR) who may be inadmissible to Canada under the Immigration and Refugee Protection Act (IRPA).

Records may be found in the following systems: the former Field Operations Support System (FOSS), the Computer-Assisted Immigration Processing System (CAIPS), the Global Case Management System (GCMS), the National Case Management System (NCMS), the Secure Tracking System (STS) and the Canadian Police Information Center (CPIC).

Document Types: Admissibility/Inadmissibility reports, forms (Vienna Convention Rights Form, Notice of Seizure, Notice of Arrest, Departure Order, Deportation Order, Exclusion Order), Warrants, case files, policies/directives, procedures, operational bulletins, manuals, discussion papers, Memoranda of Understanding (MOU), performance framework material, training strategies and course material, briefing notes, issue sheets and question period cards.

Class of Record Number:

CBSA ENF 130

- ☒ Proposal for a New Personal Information Bank
- ☐ Proposal to modify an existing Personal Information Bank - identify PIB registration number and current description:

Description: This bank describes personal information that is used in support of the processing of applications for Ministerial relief (MR), including the preparation of MR recommendations, decisions rendered and associated supporting material. Personal information may include the applicant's name, gender, contact information, biographical information, biometric information, citizenship status, credit information, nationality, marital status, names of any former spouses or common-law partners, nationality and immigration status of all family members of the applicant, whether accompanying or not, criminal checks/history, history of detention, immigration and enforcement history, date of birth, place of birth, education and training, financial information, physical attributes, employment and volunteer history, membership and association with organizations or foreign governments, police, military and paramilitary history, engagement in acts of espionage, subversion, terrorism, human smuggling, use of armed struggle or violence to reach political, religious or social objectives, human trafficking and/or money laundering, involvement in an act of genocide or in the commission of a war crime or crime against humanity, medical information, photos, travel documentation, signature, travel history, previous countries of residence, applicant and/or representative contact information and immigration identification numbers. The bank may also include applications for permanent residence and refugee status, assessments by immigration officers, removal documentation, temporary resident permits, previous findings of inadmissibility and supporting evidence, court and tribunal records, any considerations that the applicant feels would satisfy the Minister that granting Ministerial relief is not contrary to the national interest, and computer-based information (former Field Operations Support System (FOSS), Computer-Assisted Immigration Processing System (CAIPS), Case Processing System (CPS), the National Case Management System (NCMS), the Global Case Management System (GCMS), the Secure Tracking System (STS), the Canadian Police Information Center (CPIC) and e-mail).

Note: The personal information may be stored in the following internal databases: the former Field Operations Support System (FOSS); the National Case Management System (NCMS); the Global Case Management System (GCMS); and the Secure Tracking System (STS).

Class of individuals: General Public

Purpose: To administer the Ministerial relief component of the CBSA's Immigration Program, specifically in order to process applications for MR submitted under subsection 42.1(1) of the *Immigration and Refugee Protection Act* (IRPA). Information is collected under the authorities of subsections 15(1) and 16(1) of the IRPA, paragraph 28(a) of the *Immigration and Refugee Protection Regulations* (IRPR) and pursuant to new regulatory amendments to the IRPR that will be created in order to authorize the collection of specific information for the purposes of MR applications. The new regulations will also incorporate certain elements of section 10 of the IRPR, as well as specifically authorize the Minister of Public Safety and Emergency Preparedness to create an application form for MR (see Attachment 2).

Consistent Uses: Information may be disclosed to the Canadian Security Intelligence Service (CSIS) (refer to: Canada's War Crimes Program – CBSA PPU 028, Fugitive Information Bank – CBSA PPU 020, Enforcement Data System – CBSA PPU 032, Enforcement Information Index System (EIIS) – CBSA PPU 025), the Immigration and Refugee Board (IRB) (refer to: Intelligence Program – CBSA PPU 035, Canada's War Crimes Program – CBSA PPU 028, Hearings and Detentions Program – CBSA PPU 1107, Enforcement Data System – CBSA PPU 032) and Immigration, Refugees and Citizenship Canada (IRCC) (refer to: Intelligence Program – CBSA PPU 035, Canada's War Crimes Program – CBSA PPU 028, Enforcement Data System – CBSA PPU 032, Immigration Investigations Program – CBSA PPU 1403) for the purpose of conducting security reviews, hearings or investigations related to immigration legislation. Information may be disclosed to the US NCIC and to INTERPOL to confirm the accuracy of information the CBSA has on file. Information may be disclosed to CBSA inland enforcement (refer to Immigration Investigation Program – CBSA PPU 1403 and Enforcement Data System – CBSA PPU 032) for review for possible further enforcement action either under inadmissibility provisions, or for criminal proceedings initiated under the IRPA.

Information may be disclosed to parties to a dispute, hearing or proceedings or similar matters. The information may be shared with the Department of Justice for the purpose of judicial review, appeals and obtaining legal advice (Civil Proceedings and Legal Services - JUS PPU 010). Information may be shared with Courts of Law for judicial review and appeal purposes. Information may be shared with the IRB for the purpose of proceedings before the Immigration Division (Immigration Division Case Files - IRB PPU 140) and Refugee Protection Division (Refugee Protection Division Records - IRB PPU 115). The information found in the following banks may be compared with the information already obtained. Each bank has a specific purpose for the disclosure. CBSA PPU 1202 is used for the purposes of improving border management by enabling the CBSA to monitor the flow of persons entering and departing from Canada; CBSAPPU 1301 is used to administer the Removal Program and to facilitate the enforcement of removal orders; CBSAPPU 1402 is collected pursuant to the *Immigration and Refugee Protection Act (IRPA)*, the *Customs Act*, the *Customs Tariff*, the *Excise Act*, *Export and Import Permits Act* and the *Criminal Code of Canada* for the purposes of law enforcement; CBSA PPU1403 is collected pursuant to the *Immigration and Refugee Protection Act (IRPA)* for the purposes of the administration and enforcement of *IRPA* and related immigration legislation and regulations; CBSA PPU 021 is used to provide follow-up on the activities of individuals being held in the Immigration Holding Centre in the Quebec region; CBSA PPU 1107 is used to administer and provide services for the Hearings and Detentions Program; CBSA PPU 060 is used to monitor the compliance of the individual subject to a security certificate to the terms and conditions imposed by the Federal Court; CBSA PPU035 is collected pursuant to the *Customs Act*, the *Immigration and Refugee Protection Act (IRPA)*, the *Customs Tariff*, the *Excise Act*, the *Excise Tax Act* the *Export & Import Permits Act*, the *Controlled Drugs and Substances Act (CDSA)* and the *Proceeds of Crime (Money Laundering) & Terrorist Financing Act* for the purposes of obtaining information on persons who are suspected of border related illegal activities, including contraband smuggling and immigration violations; CBSAPPU 030 is used in the administration and enforcement of citizenship and immigration legislation; CBSAPPU 028 is used to provide services for the permanent resident, temporary resident, refugee and citizenship programs and activities of Citizenship and Immigration Canada relative to admissibility to Canada; CBSA ENF 105 contains records related to the Counter Terrorism Program; CBSA PPU 008 is used for the purposes of administering the Advance Passenger Information / Passenger Name Record (API/PNR) Program, which involves performing a risk assessment including a scenario based risk analysis and query for enforcement and intelligence information for individuals prior to their arrival in Canada.), IRCC (CIC PPU 042 is used to determine the eligibility of applicants for permanent residency under an economic class, as authorized under *IRPA*, and to administer and enforce program requirements; CIC PPU 009 is used to assess an individual's admissibility to Canada, and to determine his or her eligibility for referral to the Immigration and Refugee Board (IRB); CIC PPU 054 is used to administer, monitor and enforce program requirements, including the individual's compliance with his or her conditions of temporary residence and the final disposition of his or her case file; CIC PPU 050, is used to determine the citizenship status of Canadians and failed applicants for citizenship, and to facilitate the processing of applications for citizenship.), the IRB and CSIS for the purpose of administering or enforcing immigration legislation.

Retention and Disposal Standards: Personal information collected will be retained for a period of 80 years or when the individual is 100 years of age and only after the file has been closed. Furthermore records will be retained for two years following their last administrative use. Where files have been designated as historical they may be transferred to the custody and control of Library and Archives Canada; where the record has not been so designated, it shall be destroyed.

RDA Number: 2015/008

Related Class of Record Number: CBSA ENF 137, CBSA ENF 127, CBSA ENF 130

TBS Registration: To be assigned by TBS.

Bank Number: CBSA PPU 1504.

Name of Program / Activity / Service

PIA

- ☐ Proposed new Standard Personal Information Bank
- ☐ Proposal to modify an existing Standard Personal Information Bank - identify Standard PIB number and current description:

Copy and paste PIB entry from CBSA Info Source. Be sure to include the description and PIB registration number.

Legal Authority for Program or Activity:

IRPA Subsection 15(1): An officer is authorized to proceed with an examination if a person makes an application to the officer in accordance with this Act or if an application is made under subsection 11(1.01)

IRPA Subsection 16(1): A person who makes an application must answer truthfully all questions put to them for the purpose of the examination and must produce a visa and all relevant evidence and documents that the officer reasonably requires.

IRPA Section 42.1: The Minister may, on application by a foreign national, declare that the matters referred to in section 34, 35(1)(b) and (c) and subsection 37(1) do not constitute inadmissibility in respect of the foreign national if they satisfy the Minister that is not contrary to the national interest

IRPA Section 43: The regulations may provide for any matter relating to the application of this Division, may define, for the purposes of this Act, any of the terms used in this Division, and may include provisions respecting the circumstances in which a class of permanent residents or foreign nationals is exempted from any of the provisions in this Division.

IRPA Subsection 34(1): A permanent resident or a foreign national is inadmissible on security grounds for

- a) engaging in an act of espionage that is against Canada or that is contrary to Canada's interest
- b) engaging in or instigating the subversion by force of any government
- b.1) engaging in an act of subversion against a democratic government, institution or process as they are understood in Canada
- c) engaging in terrorism
- d) being a danger to the security of Canada
- e) engaging in acts of violence that would or might endanger the lives or safety of person in Canada
- f) being a member of an organization that there are reasonable grounds to believe engages, has engaged or will engage in acts referred to in paragraph (a), (b), (b.1) or (c)

IRPA Subsection 35(1): A permanent resident or a foreign national is inadmissible on grounds

- a) committing an act outside Canada that constitutes an offence referred to in sections 4 to 7 of the Crimes Humanity and War Crimes Act.
- b) Being a prescribed senior official in the service of a government that, in the opinion of the Minister Engages or has engaged in terrorism, systematic or gross human rights violations, or genocide, a war crime or a crime against humanity with the meaning of subsections 6(3) to (5) of the Crimes Against Humanity and War Crimes act; or

IRPA Subsection 18 (1) Every person seeking to enter Canada must appear for an examination to determine whether that person has a right to enter Canada or is or may become authorized to enter and remain in Canada.

Note: Prior to proceeding with the assessment it is essential that Parliamentary authority for the relevant program or activity be established. Generally, Parliamentary authority is contained in an Act of Parliament or subsequent regulations, or approval of expenditures proposed in the Estimates and authorized by an Appropriations Act. If legal authority is unclear consult your Legal Service to determine authority for the program or activity. (See question 1 of Section 5)

SECTION 2 - RISK AREA IDENTIFICATION AND CATEGORIZATION

For Section 2, check the appropriate box that describes the level of risk related to your program or activity and provide details as indicated. Please note that answering "yes" or "no" without providing explanatory details may trigger more questions from the Office of the Privacy Commissioner.

Please ensure that the details provided respond to these 4 elements:

1. **Necessary:** It must be demonstrably necessary in order to meet some specific need
2. **Effective:** It must be demonstrably likely to be effective in achieving its intended purpose. In other words, it must be likely to actually make us significantly safer, not just make us feel safer.
3. **Proportionate:** The intrusion on privacy must be proportional to the security benefit to be derived.
4. **Minimal:** and it must be demonstrable that no other, less privacy-intrusive, measure would suffice to achieve the same purpose

Type of Program or Activity

Level of Risk

Program or activity that does NOT involve a decision about an identifiable individual

☐ 1

Personal information is used strictly for statistical / research or evaluations including mailing list where no decisions are made that directly have an impact on an identifiable individual.

The Directive on PIA applies to administrative use of personal information. The Policy on Privacy Protection requires that government institutions establish an institutional Privacy Protocol for addressing non-administrative uses of personal information. *The CBSA Privacy Protocol must be implemented. Contact the ATI and Privacy Division before continuing the PIA.*

Administration of Programs / Activity and Services

☒ 2

Personal information is used to make decisions that directly affect the individual (i.e. determining eligibility for programs including authentication for accessing programs/services, administering program payments, overpayments, or support to clients, issuing or denial of permits/licenses, processing appeals, etc...).

Compliance / Regulatory investigations and enforcement

☐ 3

Personal information is used for purposes of detecting fraud or investigating possible abuses within programs where the consequences are administrative in nature (i.e. a fine, discontinuation of benefits, audit of personal income tax file or deportation in cases where national security and/or criminal enforcement is not an issue).

Criminal investigation and enforcement / National Security

☒ 4

Personal information is used for investigations and enforcement in a criminal context (i.e. decisions may lead to criminal charges/sanctions or deportation for reasons of national security or criminal enforcement).

Details: Ministerial relief is sought by a foreign national in order to obtain an exception to some of the most serious inadmissibility provisions in the IRPA, namely: security, certain provisions relating to violations of human or international rights, and organized criminality. The applicant may be, but is not required to be, physically present in Canada. Although not intended to establish or reassess inadmissibility under the IRPA, the Ministerial relief process involves analysis of information relating to very serious allegations that led to an applicant's inadmissibility, in addition to the assessment of other elements, in order to determine whether there exist exceptional factors warranting relief from that inadmissibility. A declaration of relief by the Minister removes an impediment to temporary or permanent resident status in Canada.

A final determination of inadmissibility will be a prerequisite for Ministerial relief applications following the

coming-into-force of the proposed regulatory amendments. Information relating to the grounds of inadmissibility will continue to be taken into consideration by the MRU when processing an application for Ministerial relief. Among the requests for Ministerial relief received prior to the coming-into-force of the proposed regulatory amendments, some have had formal inadmissibility determinations, and others have not. Even where an inadmissibility determination on the basis of security, human or international rights violations, or organized criminality has not been formally established, requests for Ministerial relief nevertheless involve information related to these issues.

Name of Program / Activity / Service	PIA
--------------------------------------	-----

Type of Personal Information Involved and Context	Level of Risk
Only personal information, with no contextual sensitivities, collected directly from the individual or provided with the consent of the individual for disclosure under an authorized program. For example: General licensing, or renewal of travel documents or identity documents.	<input type="checkbox"/> 1
Personal information, with no contextual sensitivities after the time of collection, provided by the individual with consent to also use personal information held by another source. For example: An application process with a requirement for independent verification of certain non-sensitive factual details.	<input type="checkbox"/> 2
Social Insurance Number, medical, financial or other sensitive personal information and/or the context surrounding the personal information is sensitive. Personal information of minors or incompetent individuals or involving a representative acting on behalf of the individual. For example: An individual's name on a particular list may reveal sensitive information on the health, financial situation, religious or lifestyle choices of that individual.	<input checked="" type="checkbox"/> 3
Sensitive personal information, including detailed profiles, allegations or suspicions, bodily samples and/or the context surrounding the personal information is particularly sensitive. For example: Personal information that reveals intimate details on the health, financial situation, religious or lifestyle choices of the individual and which, by association, reveals similar details about other individuals such as relatives.	<input checked="" type="checkbox"/> 4
<p>Details: In accordance with the planned regulatory amendments, it will be mandatory for applicants to provide basic tombstone information, including name, address, telephone number and email address, DOB, gender, immigration number, former countries of citizenship or nationality, marital status, the names of their former spouse(s) or common law partner(s), and details relating to their education, employment and international travel history. Failure to provide the above information will result in the application being returned unprocessed.</p> <p>Applicants are also asked to provide details relating to organizational affiliations, government positions held, service in military, paramilitary or police organizations (and training received), criminal history, and previous countries of residence. If the applicant used the services of a representative, the representative's personal information (including contact information) must be provided on form IMM 5746 (see attached). If the applicant used the services of an interpreter, the interpreter must attest to the accuracy of their interpretation.</p> <p>Applicants must provide the date, city, country, and circumstances under which they were previously found inadmissible under any of the following sections of the IRPA: 34(1), 35(1) and 37(1).</p>	

Program or Activity Partners and Private Sector Involvement	Level of Risk
Within the CBSA (amongst one or more programs within the CBSA)	<input checked="" type="checkbox"/> 1
With other federal institutions	<input checked="" type="checkbox"/> 2
With other or a combination of federal/ provincial and/or municipal government(s)	<input checked="" type="checkbox"/> 3

Name of Program / Activity / Service

PIA

Private sector organizations or international organizations or foreign governments

☒ 4

Details: Finalising recommendations on Ministerial relief requests may require consultation with other Government of Canada partners such as IRCC, DOJ, Public Safety and CSIS. Comments on draft recommendations from CBSA partners, if any, are taken into consideration by the CBSA MRU prior to the recommendations being disclosed to the applicant and before they are forwarded to the Minister of Public Safety for a decision to grant or deny relief. Applicants' names, date of birth and other identifiers may be disclosed in order to obtain reports from provincial criminal justice and correctional authorities where an applicant has spent time in a provincial jail or detention facility.

Duration of the Program or Activity

Level of risk

One time program or activity

☐ 1

Typically involves offering a one-time support measure in the form of a grant payment as a social support mechanism.

Short-term program

☐ 2

A program or activity that supports a short-term goal with an established "sunset" date.

Long-term program

☒ 3

Existing program that has been modified or is established with no clear "sunset".

Details: Ministerial relief is a long-term program with no "sunset" date.

Program Population

Level of Risk

The program affects certain employees for internal administrative purposes.

☐ 1

The program affects all employees for internal administrative purposes.

☐ 2

The program affects certain individuals for external administrative purposes.

☒ 3

The program affects all individuals for external administrative purposes.

☐ 4

Details: Individuals who have applied for Ministerial relief.

Technology and Privacy

6.1 Does the new or modified program or activity involve the implementation of a new electronic system, software or application program including collaborative software (or groupware) that is implemented to support the program or activity in terms of the creation, collection or handling of personal information?

☐ YES

☒ NO

6.2 Does the new or modified program or activity require any modifications to IT legacy systems and / or services?

☐ YES

☒ NO

6.3 Does the new or modified program or activity involve the implementation of one or more of

Name of Program / Activity / Service

PIA

the following technologies:

6.3.1 Enhanced identification methods:

This includes biometric technology (i.e. facial recognition, gait analysis, iris scan, fingerprint analysis, voice print, radio frequency identification (RFID), etc...) as well as easy pass technology, new identification cards including magnetic stripe cards, "smart cards" (i.e. identification cards that are embedded with either an antenna or a contact pad that is connected to a microprocessor and a memory chip or only a memory chip with non-programmable logic).

☐ YES

☒ NO

Details: If YES, describe the modifications that affect the electronic system, software or technology. Identify if a new technology is being implemented and describe how it works.

6.3.2 Use of Surveillance:

This includes surveillance technologies such as audio/video recording devices, thermal imaging, recognition devices, RFID, surreptitious surveillance / interception, computer aided monitoring including audit trails, satellite surveillance etc.

☐ YES

☒ NO

Details: If YES, describe how and where the surveillance will be used, the type of surveillance, and the number of surveillance components used.

6.3.3 Use of automated personal information analysis, personal information matching and knowledge discovery techniques:

For the purposes of the Directive on PIA, CBSA is to identify those activities that involve the use of automated technology to analyze, create, compare, cull, identify or extract personal information elements. Such activities would include personal information matching, record linkage, personal information mining, personal information comparison, knowledge discovery, information filtering or analysis. Such activities involve some form of artificial intelligence and/or machine learning to uncover knowledge (intelligence), trends/patterns or to predict behaviour.

☐ YES

☒ NO

Details: The Ministerial relief process does not require any changes to CBSA information technology systems. The process of preparing a recommendation for the consideration of the Minister is already established, and functions according to current systems. The MRU does not make use of automated person matching systems, but instead conducts manual searches of current databases that hold immigration information (NCMS, GCMS, and STS) based on an applicant's biographical data.

A YES response to any of the above indicates potential privacy concerns and risks that need to be measured and mitigated.

Personal Information Transmission

Level of Risk

The personal information is used within a closed system.

☐ 1

No connections to Internet, Intranet or any other system. Circulation of hardcopy documents is controlled.

The personal information is used in system that has connections to at least one other system.

☒ 2

The personal information is transferred to a portable device or is printed.

☒ 3

USB key, CD-Rom, laptop computer, any transfer of the personal information to a different medium.

The personal information is transmitted using wireless technologies.

☒ 4

Name of Program / Activity / Service

PIA

Details: Personal information is used by MRU officers accessing NCMS, STS and GCMS, three case management systems residing on the closed, secure CBSA network (RCNET). Officers may also access connected OGD systems through secure web portals using virtual private networks, such as CPIC.

Risk Impact to the CBSA

Level of Risk

Managerial harm.

☒ 1

Processes must be reviewed, tools must be changed, change in provider / partner.

Organizational harm.

☐ 2

Changes to the organizational structure, changes to the organizations decision-making structure, changes to the distribution of responsibilities and accountabilities, changes to the program activity architecture, departure of employees, reallocation of HR resources.

Financial harm.

☒ 3

Lawsuit, additional moneys required reallocation of financial resources.

Reputation harm, embarrassment, loss of credibility.

☒ 4

Decreased confidence by the public, elected officials under the spotlight, institution strategic outcome compromised, government priority compromised, impact on the Government of Canada Outcome areas.

Details: If personal data were breached by the MR program, the CBSA could face litigation risks. The CBSA and its partners could also suffer significant reputational harm if sensitive personal information were breached.

Risk Impact to the Individual or Employee

Level of Risk

Inconvenience.

☒ 1

Reputation harm, embarrassment.

☒ 2

Financial harm.

☒ 3

Physical harm.

☒ 4

Details: If a Ministerial relief package were to be made available to someone other than the applicant, the applicant could suffer reputational harm or embarrassment given the seriousness of the grounds of inadmissibility contained in the allegations. It is also conceivable that the applicant could suffer financial harm as a release of information could cause them to lose business or employment, as well as physical harm, since their previous actions or involvement in certain organizations, such as those operating in organized crime, could conceivably lead to acts of retribution from other groups.

SECTION 3 - ANALYSIS OF PERSONAL INFORMATION ELEMENTS

Personal Information Elements and Sub-elements

Category Of Personal Information	Personal Information Element	Personal Information Sub-Element	Format	Purpose / Necessity of Element
Name	Name	Given name(s), surname(s)/family name(s)	Paper / Electronic	To identify applicant.
Name	Aliases	Any aliases, nicknames, maiden names, or changes of name.	Paper / Electronic	To identify applicant.
Date of birth	Date of birth	Day, month, year of birth.	Paper / Electronic	To identify applicant.
Place of birth	Place of birth	City and country of birth	Paper / Electronic	To identify applicant. Required by ss.24.2(1) of the upcoming Regulations – 24.2(1)(a)
Physical attributes	Gender	Male, Female, Other	Paper / Electronic	To identify applicant. Required by ss.24.2(1) of the upcoming Regulations – 24.2(1)(a)
Citizenship status	Citizenship/Nationality	All countries of citizenship/nationality, date citizenship/nationality obtained, how citizenship/nationality was obtained, and present status.	Paper / Electronic	To identify applicant. Required by ss.24.2(1) of the upcoming Regulations – 24.2(1)(c)
Other: Language	Language(s) and dialect(s)	Language(s) and dialect(s) spoken	Paper/ Electronic	To help confirm identity and verify background details provided by the applicant.

Other: Language of preference	Official language	English, French	Paper / Electronic	To ensure fairness of processing.
Biographical information	Marital Status	Single, common-law, married, legally separated, annulled marriage, divorced, widowed, or unknown	Paper / Electronic	To identify applicant
Biographical information	Spouse, partner name(s)	Given name, surname of past or present spouse(s) or common-law partner(s).	Paper / Electronic	This information will help confirm identity of applicant. Required by ss.24.2(1) of the upcoming Regulations – 24.2(1)(a)
Other identification numbers	Canadian immigration ID number	N/A	Paper / Electronic	To identify applicant immigration file.
Educational information	Formal education/training	Name of institution(s); field(s) of study; town, city, district, region, state/province, country; level, degree, diploma or certificate obtained; and start and end dates.	Paper / Electronic	To confirm and update background details of applicant and provide information to be considered in the context of MR national interest assessment. Required by ss.24.2(1) of the upcoming Regulations – 24.2(1)(d)
Other: Inadmissibility	Inadmissibility determination	Described by ss. 34(1) – membership, engagement in act(s), and/or being a danger; paras. 35(1)(b) and/or (c) – senior officials and/or sanctions; or ss. 37(1) – organized/transnational criminality (this includes all corresponding provisions under the former <i>Immigration Act</i>).	Paper / Electronic	To determine compliance with the regulatory amendments and identify basis for which relief is being sought. Required by ss.24.2(1) of the upcoming Regulations – 24.2(1)(g)
Other: Inadmissibility	Type of refusal	Temporary or permanent resident status refusal by	Paper /	To determine compliance with regulatory amendments and identify basis for which relief is

		IRCC/visa office; or removal order issued by the IRB.	Electronic	being sought.
Other: Inadmissibility	Date, location of refusal	Date on which, and city and country where, inadmissibility decision was rendered.	Paper / Electronic	To assist with aligning the basis of inadmissibility determination with Ministerial relief submissions.
Other: Inadmissibility	Litigation status of the decision	Is the finding of inadmissibility under or subject to litigation?	Paper / Electronic	To determine compliance with the regulatory amendments.
Other: Other inadmissibility(ies)	Inadmissibility to Canada under other sections of IRPA	Reports or determinations of inadmissibility under sections of IRPA other than 34, 35, or 37 (this includes all corresponding provisions under the former <i>Immigration Act</i>).	Paper / Electronic	To confirm and update background details of applicant and provide information to be considered in the context of MR national interest assessment.
Other: Immigration history	Immigration status	Has applicant ever been refused refugee status, immigration status or a visa to Canada or any other country?	Paper / Electronic	To confirm and update background details of applicant.
Other: Immigration history	Removal history	Has applicant ever been refused admission to, or ordered to leave, Canada or any other country?	Paper / Electronic	To confirm and update background details of applicant; confirm requirements with proposed regulatory amendment (i.e. if removal order issued)
Other: Immigration history	Arrest history	Has applicant ever been sought, arrested or detained for any reason?	Paper / Electronic	To confirm and update background details of applicant, collect information on any prior or new criminal activity, and provide information to be considered in the context of national interest assessment for Ministerial relief.
Other: inadmissibility and national interest	Personal planning or advocating the use	Has the applicant ever planned or advocated the use of violence for	Paper / Electronic	To confirm and update background details of applicant, and provide information to be

	of violence	political, social, or religious motives?		considered in the context of national interest assessment for Ministerial relief.
Other: inadmissibility and national interest	Voluntary association with a group or designated regime	Was any association with a group, organization, military, paramilitary or designated regime voluntary?	Paper / Electronic	To confirm and update background details of applicant, and provide information to be considered in the context of national interest assessment for Ministerial relief.
Other: inadmissibility and national interest	Awareness of group's hostilities	Was the applicant aware of the group's involvement in hostilities?	Paper / Electronic	To confirm and update background details of applicant, and provide information to be considered in the context of national interest assessment for Ministerial relief.
Other: inadmissibility and national interest	Participation in or support of a group's hostilities	Did the applicant participate in or provide support to a group's armed hostilities?	Paper / Electronic	To confirm and update background details of applicant, and provide information to be considered in the context of national interest assessment for Ministerial relief.
Other: inadmissibility and national interest	Any association with groups involved with terrorism or subversion	Has the applicant ever been associated with a group that uses or advocates the use of armed struggle for religious, political, or social objectives, and, if so, whether the applicant was aware of the group's involvement in such activities?	Paper / Electronic	To confirm and update background details of applicant, identify any prior, new or continued association with groups posing security concerns, and provide information to be considered in the context of national interest assessment for Ministerial relief.
Other: inadmissibility and national interest	Involvement in activities of security concern and/or organized criminality	Has the applicant ever engaged in espionage, subversion, terrorism, organized crime and/or transnational crime (e.g., human smuggling, human trafficking, or money laundering)?	Paper / Electronic	To confirm and update background details of applicant, and provide information to be considered in the context of national interest assessment for Ministerial relief.
Other: inadmissibility and	Voluntariness of	Was any involvement in activities that raise security concerns	Paper /	To confirm and update background details of applicant, and provide information to be

Name of Program / Activity / Service	PIA
--------------------------------------	-----

national interest	activities	and/or in organized criminality or transnational crime voluntary?	Electronic	considered in the context of national interest assessment for Ministerial relief.
Other: inadmissibility and national interest	Complicity in war crimes or crimes against humanity	Has the applicant ever advocated or been involved in an act of genocide or in the commission of a war crime or crime against humanity?	Paper/ Electronic	To confirm and update background details of applicant, ensure applicant's eligibility for Ministerial relief, and provide information to be considered in the context of national interest assessment.
Other: inadmissibility and national interest	International Sanctions	Was the applicant ever subject to international sanctions imposed by an international group of which Canada is a member?	Paper / Electronic	To confirm and update background details of applicant, and provide information to be considered in the context of national interest assessment for Ministerial relief.
Other: inadmissibility and national interest	Employment history	Applicant to list all employers and volunteer work since the age of 16 (including all periods of unemployment, if applicable), including: name of employer/company/organization; town, city, district, region, state/province; country and country of employment; occupation/job title or description of work and beginning and end dates.	Paper / Electronic	To confirm and update background details of applicant, identify any prior, new or continued association with groups posing security concerns, and provide information to be considered in the context of national interest assessment for Ministerial relief. Required by ss.24.2(1) of the upcoming Regulations – 24.2(1)(e)
Other: inadmissibility and national interest	History of association with organizations	Applicant to list all organizations in which they have participated, or of which they were (or still are) a member, with which they were (or still are) associated, and/or which they supported, including	Paper / Electronic	To confirm and update background details of applicant, identify any prior, new or continued association with groups posing security concerns, and provide information to be considered in the context of national interest assessment for Ministerial relief.

		the dates and places of involvement (including town, city, district, region, state/province, and country), types of organizations that they supported, and applicant's titles, roles, positions and responsibilities.		
Other: inadmissibility and national interest	Government positions held	Applicant to list any positions with a government including the dates of employment, level of jurisdiction, department/branch; activities and positions held, city and country of employment, if the position involved intelligence gathering and/or analysis.	Paper / Electronic	To confirm and update details of the applicant, identify any prior, new or continued association with designated government regimes, and provide information to be considered in the context of national interest assessment for Ministerial relief.
Other: inadmissibility and national interest	Military Paramilitary, or police	Applicant to list any type of military, paramilitary or police service performed, including: whether service was voluntary or mandatory; whether there was a draft age (age required to join); the length of any mandatory service; the applicant's length of service; whether the period of service was completed (and to provide the beginning and end dates); under what circumstances the service ended; the applicant's titles, ranks, roles and responsibilities (including the	Paper / Electronic	To confirm and update background details of applicant, and provide information to be considered in the context of national interest assessment for Ministerial relief.

Name of Program / Activity / Service

PIA

		corresponding dates of promotion); the branches and units in which the applicant served; the titles, ranks and names of individuals to whom the applicant reported; the country and all locations of service; awards, medals and commendations the applicant received (including dates); disciplinary measures against the applicant (including dates); whether the applicant received any military, paramilitary or police training; whether the applicant participated in any conflicts, violence, or exchanges of weapon fire; and whether the applicant ever witnessed or participated in ill treatment of prisoners or civilians, hostage-taking, looting, or desecration of cultural or religious artifacts or buildings.		
Criminal checks/history	Criminal history	Has the applicant ever committed/been party to or been arrested for, charged with, on trial for, or convicted of a crime or offence, or subject to any arrest warrants or criminal proceedings, in any country, including Canada?	Paper / Electronic	To confirm and update background details of applicant, and provide information to be considered in the context of national interest assessment for Ministerial relief.

		Applicant to notify the CBSA of any changes to their criminal activity, charges or record; list all offences, crimes and charges; crime/offence type and code; date of crimes or offences; date charges laid; city and country of offence/charges; date and details of disposition; any sentence imposed; date any sentence served; the institution and location where sentence was served; whether any sentence was completed and, if not, provide reasons; if the applicant has ever received a pardon, had their record expunged or been deemed to be rehabilitated and, if so, provide details, including dates and pardoning/granting bodies.		
Countries of previous residence / international travel	International travel history, including countries of previous residence	Applicant to list all cities/countries in which they have resided, or to which they have travelled/visited internationally, from the age of 16 to present. Applicant will need to include the dates of travel/residence, status in the country of visit/residence, and the purpose of each travel.	Paper / Electronic	To confirm and update background details of applicant, assist in determining the applicant's whereabouts during their activities or involvement with groups/governments that led to the finding of inadmissibility, and provide information to be considered in the context of national interest assessment for Ministerial relief. International travel is required by ss.24.2(1) of the upcoming Regulations – 24.2(1)(f).

		Applicant will also need to indicate whether their travel was related to or conducted on behalf of any organizations/governments, including those associated with their inadmissibility.		
Other: National Interest documentation	National Interest evaluation including any documentation applicant wishes to submit to support their application.	Applicant may provide an account of how a declaration of relief from their inadmissibility to Canada would not be contrary to the national interest. Various – there are no restrictions on the types of information or documentation the applicant may provide to substantiate their justification for relief.	Paper / Electronic	Applicant may provide submissions with the aim of satisfying the Minister that they should be exempt from inadmissibility on the basis that it would not be contrary to the national interest. The applicant may voluntarily submit any other supporting information or documentation they wish. The absence of a precise definition of national interest allows the Minister broad discretion in weighing factors that fall under the rubrics of public safety and national security.
Contact information	Applicant's address	Street name, street number, apartment/unit, city/town, district, province/state, postal/zip code, country, P.O. box, email address, and primary and secondary telephone number (residence, cellular and/or business).	Paper / Electronic	To maintain contact with applicant. Telephone number and email address required by ss.24.2(1) of the upcoming Regulations – 24.2(1)(b).
Other: Representative	Representative/ counsel's contact information	Counsel's name, street name, street number, city, province, postal code, email, telephone	Paper / Electronic	To maintain contact with representative.

		number		
Other: Applicant declaration	Applicant declaration	Signature	Paper / Electronic	To ensure applicant understood the contents of the form. Applicant will need to declare whether they used the services of an interpreter in completing the document, and to provide the name and language as appropriate.
Other: Interpreter	Interpreter declaration	Signature	Paper / Electronic	Translator attests that documents were accurately translated and understood by applicant.
Other: Representative	Intention to appoint / cancel appointment of a representative	Check box		To indicate applicant's intention to use a representative
Other: Representative	Applicant Personal Information	Family Name		To identify individual using representative
		Given Name		To identify individual using representative
		Date of birth		To identify individual using representative
		Type of application (permanent resident, extension, citizenship, etc.)		To identify individual using representative
		CIC ID number or Unique Client ID number (if known)		To identify individual using representative
Other: Representative	Representative Personal Information	Family name		To identify representative

Name of Program / Activity / Service

PIA

		Given name		To identify representative
		Compensated / uncompensated?		To establish whether representative receives compensation for service
		Family member or friend?		To identify representative
Other: Representative	Representative Contact Information	Name of firm or organization		To confirm representative's profession
		Name of supervising lawyer (if student at law)		To confirm representative's profession
		Supervising lawyer membership ID		To confirm representative's profession
		Mailing address		To confirm representative's profession
		Phone/fax		To confirm representative's profession
		Email		To confirm representative's profession
Other: Representative	Representative Membership	Member of NGO or religious organization?		To confirm representative's profession
		Member of Immigration Consultants of Canada Regulatory Council (ICCRC), a Canadian law society, Chambres des notaires du Quebec (CNQ)		To confirm representative's profession
		Other affiliation?		To confirm representative's profession

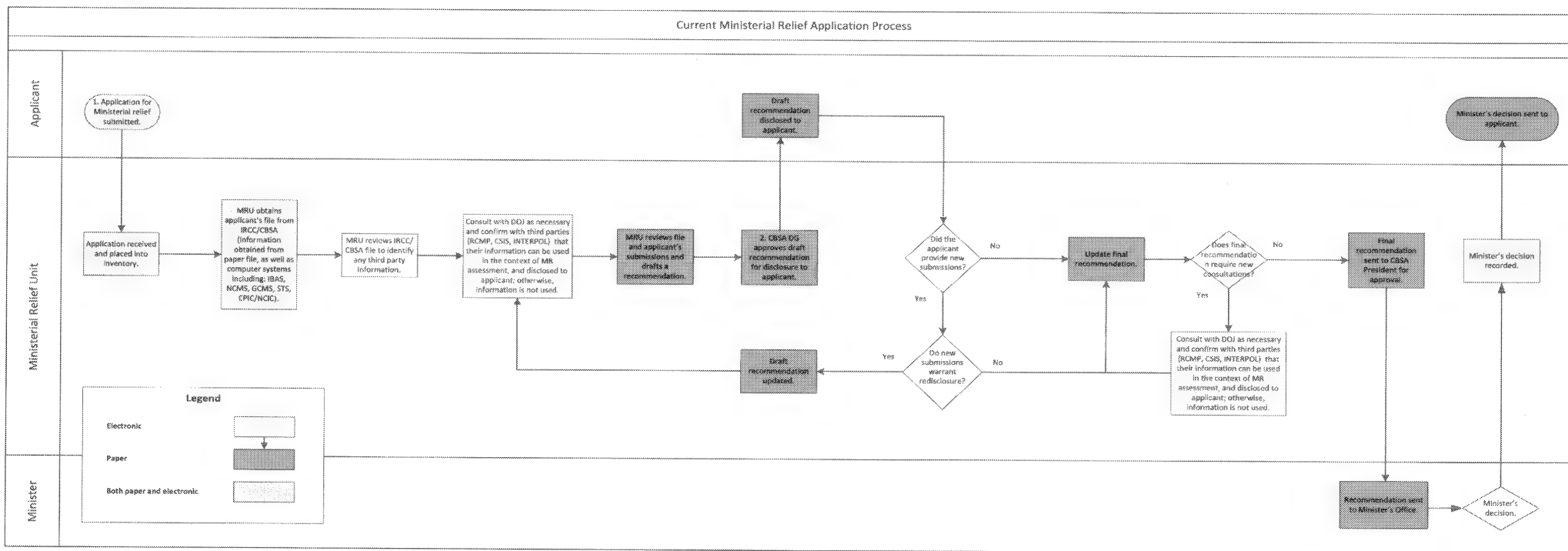
Name of Program / Activity / Service

PIA

		Will they be compensated by ICCRC?		To confirm representative's profession
		ICCRC membership number		To confirm representative's profession
		Law society membership number		To confirm representative's profession
		CNQ society membership number		To confirm representative's profession
Other: Representative	Representative declaration	Signature/date		To confirm representative's participation
Other: Representative	Cancellation of representative appointment	Name, firm or organization of representative		To cancel representative's appointment
Other: Representative	Applicant declaration	Signature/date		To confirm applicant's intentions

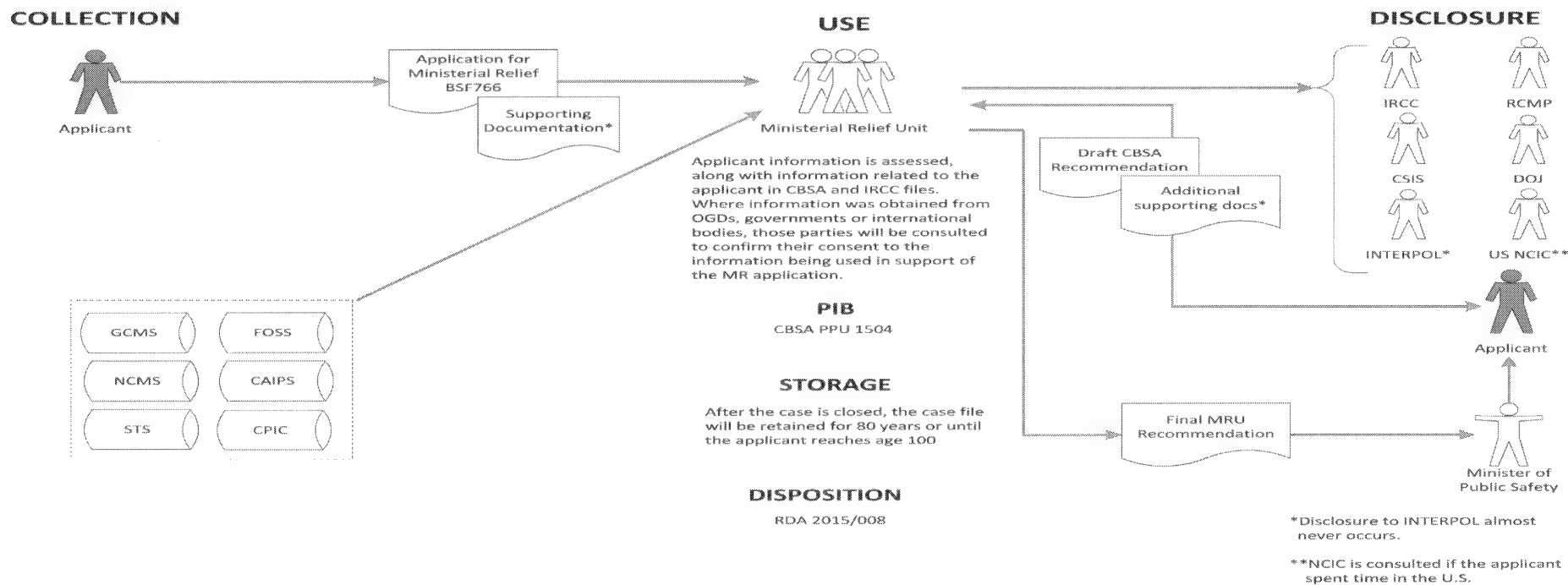
SECTION 4 - FLOW OF PERSONAL INFORMATION

4.1.1 Process Map



1. Applicants use form BSF 766E, available in PDF format from the CBSA website. They may complete and submit the form and any supporting documentation, in paper, electronic or both formats.
2. For in-Canada applicants and overseas applicants with representation in Canada, the draft recommendation package is couriered by registered mail. For overseas applicants with no representation in Canada, the package is sent via diplomatic bag and disclosed through a Canadian mission abroad.

4.1.2 Data Flow Diagram



4.2 Data Flow Model - Table

SOURCE	IDENTIFY THE SOURCE
The individual or a representative	An applicant for Ministerial relief provides personal information to the Ministerial Relief Unit (electronically, in paper format, or a combination of both), Policy Division, Enforcement and Intelligence Programs Directorate. There are no restrictions on the type of information the applicant may provide to support their application.
A federal government institution (identify from what PIB the information is obtained)	<p>Upon receipt of an application for Ministerial relief, the CBSA will obtain the applicant's immigration case file with either IRCC, the CBSA, or both. IRCC PIB CIC PPU 042 will need to be updated to reflect disclosure by the Ministerial Relief program. Similarly, CBSA PPU 035, PPU 028, PPU 032 and PPU 1403 will also need to be updated.</p> <p>If the MRU wishes to incorporate information that was collected from other federal institutions for a former proceeding under the IRPA (for example, information from the RCMP, CSC, or CSIS), the institution will be contacted to determine whether or not the source of the information consents to it being used in support of the Ministerial relief application, and to its disclosure to the applicant.¹</p>
Non federal institutions	
- Provincial Government	Reports from provincial criminal justice and correctional authorities may be sought and used if an applicant has spent time in a provincial jail or detention facility.
- Municipal Government	N/A
- Aboriginal Government / Council	N/A
- Organization of a Foreign State	Intelligence and police reports from foreign states may be used in the context of Ministerial relief

¹ Apart from requesting updates where relevant information may no longer be accurate, the Ministerial relief Unit does not seek out additional information relating to an applicant that is not already part of the applicant's case files related to the immigration continuum, or provided by the applicant in the context of the application.

Name of Program / Activity / Service

PIA

	applications, where that information is on the file obtained by the Ministerial Relief Unit, and where the source of the information permits disclosure to the applicant. For example, the CBSA may seek information from the U.S. NCIC if the applicant lived in the U.S.
- International Organization	Reports from INTERPOL and similar organisations may be used in the context of Ministerial relief applications, where that information is on a file or included in records obtained by the Ministerial Relief Unit, and where the organization permits disclosure to the applicant. ²
Private Sector	
- Located in Canada and Canadian Owned	N/A
- Located in Canada and Foreign Owned	N/A
- Located abroad and Canadian Owned	N/A
- Located abroad and Foreign Owned	N/A

4.3 Internal Use and Disclosure

Where will the information circulate within the CBSA? Identify any related programs or activities and personal information banks as identified in the CBSA Info Source chapter.

Program	Personal information bank
Immigration Investigations Program	Organized Crime Data Bank (OCS) CBSA-PPU-030 Information contained in this bank may be used in the administration and enforcement of citizenship and immigration legislation. The authority to collect personal information is authorized by sections 5(1) of the Canada Border Services Act; sections 11(1), 12.1(1), 13(a)(b), 98(1), 99(1) and 101 of the Customs Act; Sections 15(1) and 18(1) of the Immigration and Refugee Protection Act as well as sections 12(1) and 18(1) of the Proceeds of Crime (Money Laundering) and Terrorist Financing Act.

4.4 External Use and Disclosure

Where will the information circulate outside the CBSA? This includes any disclosure made to:

The individual or a representative	A disclosure package consisting of a draft MR recommendation and supporting records
------------------------------------	---

² In practice, the MRU almost never seeks applicant information from international sources.

Name of Program / Activity / Service	PIA
--------------------------------------	-----

	(redacted if necessary) is provided to the applicant and/or their representative.
A federal government institution	<p>CSIS PIB PPU 005 contains information Collected under section 15 of the <i>CSIS Act</i> to provide security assessments pursuant to section 13 or advice pursuant to section 14 of the <i>Act</i>. Pursuant to sections 19(2), 13 and 14 of the <i>CSIS Act</i>, CSIS may disclose information or may match information in the preparation of a domestic or foreign security assessment or in providing advice pertinent to the <i>Citizenship Act</i> or <i>Immigration and Refugee Protection Act</i></p> <p>RCMP PIB PPU 005, contains information Compiled in the administration or enforcement of the law and in the detection, prevention, or suppression of crime generally and is collected in accordance with section 18 of the <i>RCMP Act</i> and section 17 of the <i>RCMP Regulations</i>.</p> <p>IRCC PIB PPU 042 contains information that is used to determine the eligibility of applicants for permanent residency under an economic class, as authorized under <i>IRPA</i>, and to administer and enforce program requirements. Select information may be shared with the <i>CBSA</i> for the administration and enforcement of immigration legislation or for law enforcement purposes.</p> <p>DOJ contains information in order to enable the Department of Justice Canada to carry out its duties as legal advisor to the federal government pursuant to sections 4 and 5 of the <i>Department of Justice Act</i>. This bank contains information relating to civil legal proceedings and legal services provided to all federal departments and most government agencies and institutions.</p> <p>Public Safety (Ottawa) PIB PPU 026 is used to support the Minister, the Deputy Minister, and their officials in the exercise of their statutory duties, powers and functions; in carrying out such other national security and related law enforcement responsibilities as may be assigned to them; and in fulfilling</p>

Name of Program / Activity / Service	PIA
	<p>their obligations to manage, and be accountable to Parliament for, the national security policies and programs of the Portfolio. Information relating to threats to the safety of persons or property or to the security of Canada may be disclosed to officials of the Government of Canada, to officials of other levels of government in Canada, and to such other persons (including law enforcement agencies) as the Minister may determine are either subject to such a threat, or are in a position to assist the Government of Canada in the detection, prevention or suppression of any such threatening activities.</p>
Non-federal institutions and private sector	
<ul style="list-style-type: none"> - Provincial Government 	<p>Applicants' names, date of birth and other identifiers may be disclosed in order to obtain reports from provincial criminal justice and correctional authorities where an applicant has spent time in a provincial jail or detention facility.</p>
<ul style="list-style-type: none"> - Municipal Government 	<p>N/A</p>
<ul style="list-style-type: none"> - Aboriginal Government / Council 	<p>N/A</p>
<ul style="list-style-type: none"> - Organization of a Foreign State 	<p>Applicant's name, date of birth and other identifiers may be disclosed to the FBI's National Crime Information Center (if individual spent time in the U.S.) to obtain information on crimes committed by the applicant in the U.S. (Bridgeport, West Virginia, U.S.)</p>
<ul style="list-style-type: none"> - International Organization 	<p>Through the CBSA National Security Screening Division, the applicant's name, date of birth and gender may be disclosed to INTERPOL to obtain information on international wanted person alerts ("red notices"). (Lyon, France)</p>
Private Sector	
<ul style="list-style-type: none"> - Located in Canada and Canadian Owned 	<p>N/A</p>
<ul style="list-style-type: none"> - Located in Canada and Foreign Owned 	<p>N/A</p>
<ul style="list-style-type: none"> - Located abroad and Canadian Owned 	<p>N/A</p>
<ul style="list-style-type: none"> - Located abroad and Foreign Owned 	<p>N/A</p>

4.5 Retention / Storage

Where will the information be stored or retained? Identify all organizations that will store the information. This includes duplicates of the databases containing the personal information or any back-ups.

A federal government institution	CBSA, Ministerial Relief Unit, Ottawa; secure cabinet (DASCO), and Top Secret safe. Records of the outcome of the decision are entered into NCMS, and may be entered into GCMS. Applicant submissions and a consolidated copy of existing immigration information relating to the applicant are stored as hard copies and electronically on the CBSA internal network.
A Federal Records Centre	N/A
Non federal institutions and private sector	
- Provincial Government	N/A
- Municipal Government	N/A
- Aboriginal Government / Council	N/A
- Organization of a Foreign State	N/A
- International Organization	N/A
Private Sector	
- Located in Canada and Canadian Owned	N/A
- Located in Canada and Foreign Owned	N/A
- Located abroad and Canadian Owned	N/A
- Located abroad and Foreign Owned	N/A

4.6 Other Possible Considerations

Identify the areas, groups and individuals who access and handle the personal information:

Identify the areas / groups / divisions who are allowed to access and handle the personal information collected for the program or activity. Also, identify where these areas or groups are located (i.e. national capital region, within a province, in a foreign country, or several locations if tele-working) as well as the location of the personal information to uncover any potential trans-border or inter-jurisdictional issues. Where reasonable to do so, by virtue of the size of the organization or the number of individuals, identify individual positions rather than the work area or group.

Name of Program / Activity / Service

PIA

The CBSA responsible for program or activity:

Identify Groups or Areas / or Divisions	Positions who have access or use the personal information (where appropriate)	Geographical Location
MRU, Policy Division, Enforcement and Intelligence Program Directorate (EIPD)	Staff of up to 12 individuals including manager.	National Capital Region
Director's Office, Policy Division (EIPD)	Director Support Staff	National Capital Region
Director General's Office (EIPD)	Executive Director Director General Support Staff	National Capital Region
Vice President's Office	Vice President Support Staff	National Capital Region
President's Office	President Support Staff	National Capital Region
Minister's Office	Minister Support Staff	National Capital Region
Legal Services	Department of Justice lawyer assigned to review decision	National Capital Region

Other federal government Institution responsible for program or activity: (one table per institution):

N/A		
N/A		
N/A		

Non Federal Institution or Private Sector: 'name': (one table per institution)

N/A		
N/A		
N/A		

SECTION 5 - PRIVACY COMPLIANCE ANALYSIS

1. Legal Authority For Collection Of Personal Information (if unsure, consult with Legal Services)

Has a legal authority been identified for the collection of personal information for this program or activity?

Statutory reference: Section 4 of *Privacy Act* (Section 4 has been interpreted to mean that a legal authority must be established for a collection of personal information, but section 4 does not provide legal authority for such a collection).

Policy reference: Section 6.2.6 of *Directive on Privacy Practices*

Yes

- 1.1 ☒ Specify the legal authority and briefly explain its connection to the program or activity or how it permits the collection of the personal information:

****Ensure that the legal authority to collect the personal information is cited in the relevant PIB and in "Section 1 – Overview and PIA Initiation" above.**

The Canada Border Services Agency (CBSA) will collect the personal information on the form under the authorities of subsections 15(1) and 16(1) of the *Immigration and Refugee Protection Act* (IRPA), and paragraph 28(a) of the *Immigration and Refugee Protection Regulations* (IRPR) and pursuant to new regulatory amendments to the IRPR that will be created in order to authorize the collection of specific information for the purposes of Ministerial relief applications. This new regulations will also incorporate certain elements of section 10 of the IRPR, as well as specifically authorize the Minister of Public Safety and Emergency Preparedness to create an application form for Ministerial relief (see Attachment 2).

The personal information is being collected in order to process applications for MR, which are decided upon by the Minister of Public Safety and Emergency Preparedness (the Minister) pursuant to section 42.1(1) of the IRPA.

- 1.3 ☒ Is the personal information collected directly related to an operating program or activity?

Details: The information is collected in the context of a person seeking an exception from a finding of inadmissibility by having submitted an application to the CBSA for Ministerial relief. The information provided by the applicant, and derived from the applicant's consolidated immigration case file are important as they provide the CBSA with the necessary information from which to draft a recommendation, and for the Minister's subsequent decision.

→ Continue to Question 2

No

- 1.3 ☐ If there is no legal authority for the collection of personal information, it cannot be collected. Please consult your legal advisor to determine if there is authority to proceed with the program or activity.

****The PIA process must not continue without this key information.****

Name of Program / Activity / Service

PIA

2. Necessity To Collect Personal Information

Is each element and sub-element of personal information collected or to be collected necessary to administer the program or activity?

Statutory reference: Section 4 of *Privacy Act*

Policy reference: Sections 6.1.1, 6.1.3, 6.1.4, 6.2.7 and 6.2.8 of *Directive on Privacy Practices*

YES

- 2.1 ☒ Ensure that all personal information necessary to administer the program or activity is listed in the relevant PIB.

****Personal Information Bank (PIB) should be found within "Section 1 – Overview and Initiation" above****

- 2.2 ☒ AND, implement controls and procedures to ensure the CBSA does not collect more personal information than is necessary for the identified program or activity and that a continuing need exists for that information or its collection.

****Ensure to provide the "controls and procedures" as an annex to this PIA****

- 2.3 Are secondary uses contemplated for the information collected?

****Treasury Board defines a "Secondary Use" as a purpose that is not consistent with the original purpose of the collection.****

- ☐ YES ☒ NO (Continue to Question 3)

****If you've selected "Yes" to Question 2.3 above, please note that Consent is required for all "Secondary Uses". Please ensure that a "Consent Statement" is created. Please refer to "4. Direct Collection - Notification and Consent (as appropriate)" below for the information required in a "Consent Statement".****

- 2.3.2 If not, is there authority for the use or disclosure of the personal information?

****Please ensure that the Legal Authority identified above allows for all uses and disclosures of the personal information.****

- ☒ YES ☐ NO

→ Continue to Question 3

NO

- 2.3 ☐ Review the proposed elements and sub-elements of personal information outlined in "Section 3 – Analysis of Personal Information Elements" to identify those that are "necessary" and not merely useful. Document any changes.

3. Authority For the Collection, Use or Disclosure Of the Social Insurance Number

Is the collection of the Social Insurance Number (SIN) necessary to administer the program or activity?

Statutory reference: Section 4 of *Privacy Act*

Policy reference: Section 6.2.13 of *Policy on Privacy Protection* and sections 6.1.1 and 6.2 to 6.4 of *Directive on Social Insurance Number*

Also see "Guidance for Preparing Information-Sharing agreements Involving Personal Information" and "Taking Privacy into Account Before making Contracting Decisions"

Name of Program / Activity / Service

PIA

YES

3.1 ☐ Collection of the SIN must be in compliance with the *Directive on Social Insurance Number* (please check all appropriate boxes below):

3.2 ☐ State legal authority for collecting the SIN:

OR, in the absence of a legal authority to collect the SIN:

3.3 ☐ Establish explicit authority through legislative amendment(s).

3.4 ☐ Establish legal authority as outlined in the *Directive on Social Insurance Number*.

AND, if disclosure of the SIN by the CBSA is to occur on a routine or systematic basis

3.4.1 ☐ to another federal institution that is authorized to collect it, or to another level of government, establish an agreement or arrangement that includes specific provisions to limit the use of the SIN.

3.4.2 ☐ to a contractor or other external service provider, establish a contract that includes specific provisions to limit the use of the SIN.

3.5 ☐ AND, ensure that the relevant **PIB** for the program or activity states the authority under which the SIN is collected and the purpose for which it is used.

→ Continue to Question 4

NO

3.6 ☒ The SIN is not necessary and it will not be collected, used or disclosed to administer the program or activity.

→ Continue to Question 4

4. Direct Collection - Notification and Consent (as appropriate)

Is personal information collected directly from the individual to whom it relates?

Statutory reference: Sections 4 and 5 of *Privacy Act*

Policy reference: Sections 6.1.1, 6.2.6 and 6.2.9 to 6.2.13 of *Directive on Privacy Practices* and section 6.1.2 and 6.4.1 of *Directive on Social Insurance Number*

YES

4.1 ☒ A "**Privacy Notice**" (adapted for either verbal or written communications) must be provided to the individual at the time of collection and it must include the following elements:

- a) The purpose and authority for the collection
- b) Any uses or disclosures that are consistent with the original purpose.
- c) Any uses or disclosures that are not related to the original purpose

(This element need only be included when additional uses or disclosures on a regular basis are contemplated at the time of collection for a purpose other than the original purpose or a consistent use, in which case a "**Consent Statement**" may need to be added to the "**Privacy Notice**" – see below for "**Consent Statement**" elements.)

- d) Any legal or administrative consequences for refusing to provide the personal information

Name of Program / Activity / Service

PIA

e) That the "individual to whom the information relates" has rights of access to, correction of and protection of personal information under the *Privacy Act*.

f) A reference to the PIB for the program or activity

(This element need only be included when the notice is to be given to the individual in writing.)

****For a copy of the CBSA Privacy Notice and Consent Statement template, contact the ATI and Privacy Division.****

g) Why the SIN is collected, how it will be used and the consequence of not providing it.

(This element need only be included when the SIN is being collected – refer to "3. Authority For the Collection, Use or Disclosure Of the Social Insurance Number" above.)

AND, add a "Consent Statement" to the "Privacy Notice" as appropriate, if the personal information is to be used or disclosed for a purpose other than the original purpose (Secondary Use) or a consistent use, or, to authorize indirect collection of personal information.

4.2 ☒ The "Consent Statement" must include the following elements:

a) The purpose of the consent and the specific personal information involved.

b) In the case of indirect collections, the sources that will be asked to provide the information.

(This element need only be included when personal information is to be collected from another source e.g., person or organization with the consent of the individual)

c) Uses and disclosures that are not consistent with the original purpose of the collection and for which consent is being sought.

(This element need only be included when the individual's consent is sought for a secondary use or disclosure that is not consistent with the original purpose for which the information is collected. To find out if the individual's consent is necessary for such a use or disclosure, please consult the ATI and Privacy Division)

d) Any consequences that may result from withholding consent.

e) Any alternatives to providing consent

****For a copy of the CBSA Privacy Notice and Consent Statement template, contact the ATI and Privacy Division****

4.3 ☒ AND, implement controls and procedures to ensure that the CBSA keeps a record documenting whether or not an individual provided consent when it was sought, including a record documenting any withdrawal of consent when applicable.

****Ensure to provide the "controls and procedures" as an annex to this PIA****

Additional Consent Considerations (s. 77(1)(m) of the *Privacy Act*):

☒ Standards and mechanisms are in place to ensure that the individual has capacity to give consent.

****Ensure to provide the "standards and mechanisms" as an annex to this PIA****

→ Continue to Question 5

NO

4.4 ☐ The personal information necessary for the program or activity is not collected directly from the individual. It is collected indirectly, for example, from another program within the CBSA, or from

another institution, government or third party.

→ Continue to Question 5

5. Indirect Collection - Consent or Authority Under Sec. 10 of Privacy Regulations

Is personal information collected indirectly from another source with the informed consent of the individual to whom it relates, or from a person authorized to act on behalf of the individual pursuant to section 10 of the Privacy Regulations?

Statutory reference: Sections 4 and 5 of *Privacy Act* and section 10 of *Privacy Regulations*

Policy reference: Sections 6.1.1, 6.2.6 and 6.2.9 to 6.2.13 of *Directive on Privacy Practices* and sections 6.1.2 and 6.4.1 of the *Directive on Social Insurance Number*

YES

- 5.1 ☒ The notice and consent requirements stated at Question 4 apply. Please provide the "Privacy Notice" and/or "Consent Statement" below:

****For a copy of the CBSA Privacy Notice and Consent Statement template, contact the ATI and Privacy Division****

- 5.2 ☒ AND, implement controls and procedures to ensure the CBSA keeps a record documenting whether or not an individual provided consent when it was sought, including a record documenting any withdrawal of consent when applicable.

****Ensure to provide the "controls and procedures" as an annex to this PIA****

- 5.3 ☒ AND, if information is being collected from persons authorized to act on behalf of minors, incompetents or individuals who have been deceased for less than 20 years, implement appropriate mechanisms to ensure that such persons are authorized to act on behalf of individuals who do not have the capacity to provide consent.

****Ensure to provide the "mechanisms" as an annex to this PIA****

→ Continue to Question 6

NO

- 5.4 ☐ → Continue to Question 6

6. Indirect Collection - Without Notification and Consent

Is personal information collected from another source without notice to or consent from the individual to whom the information relates?

Statutory reference: Sections 4, 5, 7 and 8 of *Privacy Act* and section 10 of *Privacy Regulations*

Policy reference: Sections 6.2.6 and 6.2.9 to 6.2.13 of *Directive on Privacy Practices*, section 6.2.15 of the *Policy on Privacy Protection* and sections 6.3.2 and 6.3.3 of *Directive on Privacy Impact Assessment*

YES

Name of Program / Activity / Service

PIA

6.1 ☐ Where information is collected indirectly under any of the following circumstances without notice to, or consent from, the individual to whom it relates, please check the applicable boxes and explain as requested:

☐ a) The collection is a result of a disclosure to the CBSA under subsection 8(2) of the *Privacy Act*. State the applicable paragraph(s) of subsection 8(2) and provide a brief explanation for each:

Details: (This information is mandatory)

☐ b) Direct notification of the individual might result in the collection of inaccurate information, or might defeat the purpose or prejudice the use for which the information is collected. Briefly explain why notice is not provided: (For example, certain kinds of lawful investigation might be jeopardized if the investigators were required to notify the individuals who were the subjects of the investigations before collecting information indirectly from other sources.)

Details: (This information is mandatory)

☐ c) The information involved in the program or activity is to be used solely for a non-administrative purpose in which no decisions are made about the individuals to whom the information relates. (This includes research, statistical, audit or evaluation purposes.)

6.2 ☐ AND, if any of the circumstances in a) b) or c) is applicable, ensure that it is reflected in the relevant PIB.

6.3 ☐ AND, if the information is to be used solely for a non-administrative purpose (box c above has been checked), ensure that the requirements under sections 6.3.2 and 6.3.3 of the *Directive on Privacy Impact Assessment* have been met, and that the decision of the official responsible for section 10 of the *Privacy Act* to proceed with a CBSA PIA for the program or activity has been adequately documented in the description of the program or activity in "Section 1 - Overview and PIA Initiation" of the CBSA PIA.

6.4 ☐ OR, if none of the circumstances in a) b) or c) is applicable, then the personal information must be collected directly from the individual, or indirectly with the consent of the individual. Please review the responses to Questions 4 and 5 and ensure that the "Privacy Notice" or the "Consent Statement" includes all of the required elements within Question 4.

→ Continue to Question 7

NO

6.5 ☒ All personal information is collected directly from the individual to whom it relates, or from another source with notice to, or consent from, the individual or a person authorized to act on behalf of the individual (see Questions 4 and 5 above). → Continue to Question 7

7. Retention and Disposal of Personal Information

Has Library and Archives Canada approved a records retention and disposal schedule that applies to the personal information? (Consult Information Management officials to determine the authority to retain and dispose the personal information and provide the relevant details below.)

Statutory reference: Section 12 of *Library and Archives Canada Act*, sections 6, 10 and 11 of *Privacy Act* and section 4 of *Privacy Regulations*

Policy reference: Sections 6.1.3, 6.2.11 to 6.2.13 and 6.2.23 of *Directive on Privacy Practices*

YES

- 7.1 ☒ Please identify the Record Disposition Authority (RDA) and describe the retention and disposal schedule: (For example, RDA Number: 79/002, records are retained for 10 years -- active for five and dormant for five. Destruction through agreement with Library and Archives Canada.)

Details: RDA Number 2015/008. After the applicant's case file is closed, it will be retained by the CBSA for 80 years or until the applicant reaches age 100; then destroyed. If the file has been designated as having enduring value, it will be transferred to the control of Library and Archives Canada. The reason for this long retention period is that the IRPA does not preclude foreign nationals from reapplying for Ministerial relief even when the Minister has previously denied them relief on one or more occasions. Each time, an applicant's past submissions and statements given to government officials over the years, as well as any relevant historical records such as previous decisions (including any prior MR disclosures and decisions) must be reviewed and provided to the Minister in order for the Minister to render an informed decision that is legally sustainable.

- 7.2 ☒ AND, implement controls and procedures to ensure that personal information used to make a decision that directly affects an individual will be retained for a minimum of two years after the last administrative action or, where a request for access to the information has been received, until such time as the individual has had the opportunity to exercise all his/her rights under the Act. (For example, the information must be retained for at least two years after the CBSA ATI and Privacy Division responded to the request. If the requestor complains to the Privacy Commissioner, the information must be retained for at least two years following the Commissioner's finding on the complaint. If the finding is reviewed by the Federal Court, then the information must be retained for at least two years after that review is completed, and so on.)

****Ensure to provide the "controls and procedures" as an annex to this PIA****

- 7.3 ☒ AND, if the CBSA intends to dispose of personal information that has been used for an administrative purpose prior to the expiration of the two-year minimum retention standard established by the *Privacy Regulations*, it must obtain the consent of the individual to whom the information relates before doing so. (This may occur if, for example, within the two year period it is determined that the information is incorrect and that the most appropriate means of correction is disposal, or if the information is no longer required. The consent of the individual to dispose of the personal information must be obtained in writing.)
- 7.4 ☒ AND, the CBSA must cite the RDA number, the retention period and the disposition standards for the personal information in the relevant PIB.

→ Continue to Question 8

NO

- 7.5 ☐ Provide a Records Disposition Submission to Library and Archives Canada describing the records containing the personal information for which the institution requires a RDA.
- 7.6 ☐ AND, obtain a RDA from Library and Archives Canada to allow the CBSA, under certain conditions, to dispose of records that no longer have operational utility for the program or activity.
- 7.7 ☐ AND, ensure that all the other applicable requirements listed under "YES" at Question 7 are met.

→ Continue to Question 8

8. Accuracy Of Personal Information

Will measures be adopted to ensure that personal information used by the CBSA for an administrative purpose is as accurate, up-to-date and complete as possible?

Statutory reference: Sections 6, 10 and 11 of *Privacy Act* and sections 10 and 11 of *Privacy Regulations*

Policy reference: Sections 6.1.1 and 6.2.9 to 6.2.16 of *Directive on Privacy Practices*

YES

8.1 ☒ Please check any of the following measures that will be adopted to ensure accuracy of the personal information and provide details as requested:

8.1.1 ☒ Personal information will be collected directly from the individual to whom it relates or it will be validated with the individual or a person authorized to act on behalf of the individual.

8.1.2 ☒ A data-matching process will be used to verify the accuracy of personal information against a "reliable source" (within or outside the CBSA) where this is authorized, or where consent was obtained.

Details: Data matching between the applicant's submissions and CBSA records will be done by matching the biographical and case data provided by the applicant to any already existing immigration information in IRCC or CBSA case files relating to the applicant. These case files may also contain information from third parties. Information from third parties collected for the purposes of administration of the IRPA will be used in the context of Ministerial relief if the third parties agree to the use of their information for that purpose, and to its disclosure to the applicant. Information other than that which was provided directly by the applicant, and that is used in the context of the Ministerial relief application, is disclosed to the applicant. The applicant has the opportunity to make additional submissions, including consideration. Reconciliation of the information from an application for Ministerial relief with existing case files can be achieved by matching available data elements such as: name, date of birth, country of birth, country of citizenship, client identification number, and case details.

8.1.3 ☐ In cases where direct collection or consent is not feasible, the CBSA will obtain information from trusted sources (public or private) and verify accuracy against existing personal information before use.

Details: *Identify the sources and procedures to be used to check the accuracy of the information*

8.1.4 ☐ Technological methods will be used to identify errors and discrepancies.

Details: *Describe the technological methods used*

8.1.5 ☐ Other

Specify: *(This information is mandatory)*

8.2 ☒ AND, if measures are adopted other than "direct collection or validation with the individual or with a

person authorized to act on behalf of the individual", the CBSA must implement appropriate controls and procedures to ensure that:

- a) the technique(s) and the specific source(s) used to validate or update the personal information are documented;
- b) individuals are given the opportunity, whenever possible, to request correction of any inaccurate personal information before the information is used in a decision-making process that affects them;
- c) personal information can only be modified or corrected by those within the CBSA who have the authority to do so;
- d) when personal information is corrected or annotated, the record of personal information indicates the date of the last correction or annotation and the source of the information used to make the correction or annotation; and
- d) when personal information is corrected or annotated, other authorized holders of the information are notified about the correction or annotation and that all copies of the information in the possession of the CBSA are corrected / annotated.

8.3 ☒ AND, if appropriate, ensure that the "Privacy Notice" or "Consent Statement" and the relevant PIB are amended to identify the data-matching activity including the source(s).

→ Continue to Question 9

NO

8.4 ☐

Explain why such measures will not be adopted: (This information is mandatory)

→ Continue to next Question 9

****Ensure to provide all relevant "controls and procedures" implemented as a result of the above requirements as an annex to this PIA****

9. Use Of Personal Information

Will the personal information collected for the program or activity be used solely for the original purpose for which it was obtained or compiled, a use consistent with that purpose, or a purpose for which the information was disclosed to the institution pursuant to subsection 8(2) of the Privacy Act?

Statutory reference: Sections 5 and 7 to 11 of *Privacy Act*

Policy reference: Sections 6.1.1, 6.1.9, 6.2.9 to 6.2.13 and 6.2.17 of *Directive on Privacy Practices*, section 6.2.15 of *Policy on Privacy Protection* and Section IV of Appendix C of *Directive on Privacy Impact Assessment*

YES

- 9.1 ☒ Implement controls and procedures to ensure that access to the personal information for such purposes will be limited to authorized individuals who need to know the information to perform their official duties. (Applications for Ministerial relief are processed by analysts with the CBSA's Ministerial Relief Unit, reviewed by the unit manager and division director prior to being forwarded to the Director General, Vice President and Deputy Head levels for review. Departmental Legal Services may also be involved in reviewing the draft recommendation to

Name of Program / Activity / Service

PIA

ensure legislative compliance, and the relevant supporting documentation, at various stages throughout the drafting and approval of the recommendation to the Minister.)

9.2 ☒ AND, ensure that the "Data Flow Diagram" or "Data Flow Tables" completed for "Section 4 – Flow of Personal Information" of the CBSA PIA identify the areas, groups and individuals (e.g., the positions) within the CBSA who have a need-to-know to access to or handle the personal information, including their geographical location and where the personal information will be stored or retained. (See Section IV of Appendix "C" of *Directive on Privacy Impact Assessment* for a list of elements that must be included in the data flow diagram or data flow tables.)

9.3 ☐ AND, if the purposes for which the personal information is used includes any use(s) of the information for a non-administrative purpose, (such as research, statistical, audit and evaluation purposes) the CBSA will adhere to the requirements and principles in the **CBSA Privacy Protocol For Non-Administrative Purposes** (2012), in accordance with section 6.2.15 of the *Policy on Privacy Protection*, to address any impact that such non-administrative uses may have on privacy.

→ Continue to Question 10

****Ensure to provide the "controls and procedures" as an annex to this PIA****

NO

9.4 ☐ Identify below any other uses of the personal information, in other words, any routine uses that are not directly related to the purpose of the collection, or, which are not consistent with that purpose or for which the information was disclosed to the CBSA pursuant to subsection 8(2) of the *Privacy Act*:

Detail: (This information is mandatory)

9.5 ☐ AND, ensure that these other uses are reflected in the relevant **PIB**. (In accordance with subsection 9(1) of the *Privacy Act*, if these other uses are not described in the PIB in CBSA Info Source, the CBSA is required to record each use on the individual's file. Describing them in the PIB is, therefore, a far more efficient practice – see Question 11.)

9.6 ☐ AND, include a description of these other uses in the "Privacy Notice" or "Consent Statement", as appropriate,

☐ AND, ensure the all the other applicable requirements listed under "YES" at Question 9 are met.

→ Continue to Question 10

10. Disclosures Directly Related to the Administration of the Program or Activity

Will personal information be disclosed for purposes directly related to the administration of the program or activity? (This includes, for example, disclosures to other programs within the CBSA, other federal institutions, other governments, international organizations, private sector organizations or individuals.)

Statutory reference: Sections 5 and 8 to 11 of *Privacy Act*.

Policy reference: Sections 6.2.10, 6.2.11 and 6.2.13 of *Policy on Privacy Protection*, sections 6.2.1 to 6.2.3 of *Directive on Social Insurance Number*, sections 6.1.9, 6.2.9 to 6.2.13 and 6.2.15 to 6.2.20 of *Directive on Privacy Practices* and section IV of Appendix "C" of *Directive on Privacy Impact Assessment*)

Also see "Guidance for Preparing Information-Sharing agreements Involving Personal Information" and "Taking Privacy into Account Before making Contracting Decisions"

YES

- 10.1 ☒ Please check all applicable boxes below and, for each disclosure, identify the name of the organization or third party to which personal information will be disclosed. If it is disclosed within the CBSA, please identify the branch and the program or activity.

- 10.1.1 ☒ Within the CBSA for another program or activity

Detail: Information may be used to support other immigration enforcement processes. Should the applicant disclose new information that demonstrates misrepresentation on a previous application that lead to obtaining of status in Canada, efforts to vacate the previous decision may commence.

- 10.1.2 ☒ Other federal government institutions

Detail: Other federal government institutions are contacted when information originating with those departments is within the case file of a person seeking Ministerial relief, and consent from the originators of that information must be secured for the information to be used in support of drafting the Ministerial relief recommendation. Other federal government institutions are only contacted with respect to the information that those departments provided either to IRCC or CBSA in the past. Generally, third party information is not disclosed to other federal government institutions that are not the originators of the information. Occasionally, in order to prevent inadvertent disclosure, CSIS may be engaged to conduct a review when there is concern that a third party document (e.g. IRCC report) contains national security-privileged information. The Ministerial recommendation and supporting documents (including the applicant's submissions and the relevant information from the immigration case files may be provided to DOJ for review to ensure compliance with administrative law and relevant jurisprudence. DOJ is engaged on an as-needed basis, and could be asked to re-review the recommendation for the same applicant, if sufficiently significant changes are made or novel arguments are raised following disclosure of the recommendation to the applicant.

- 10.1.3 ☒ Provincial, territorial or municipal governments institutions

Detail: Reports from provincial criminal justice and correctional authorities may be sought and used if an applicant has spent time in a provincial jail or detention facility.

- 10.1.4 ☒ Foreign government institutions and entities thereof

Detail: The identity of applicants who have spent time in the U.S. may be disclosed to the FBI's NCIC to ascertain whether the applicant has a criminal record there.

- 10.1.5 ☒ International organizations

Detail: Information originating with INTERPOL may be present on an immigration (IRCC or CBSA) case file. Should the Ministerial Relief Unit wish to incorporate that information into a recommendation, INTERPOL is contacted to ensure that it consents to the use and

Name of Program / Activity / Service

PIA

disclosure of its information. If such consent is not obtained, the information is not taken into consideration in drafting the recommendation. In practice, the CBSA rarely has in its possession, or discloses, applicant information from international sources.

10.1.6 ☐ The private sector (e.g., contractor or other external service provider)

Detail: *(This information is mandatory)*

10.1.7 ☐ Other

Detail: *(This information is mandatory)*

10.2 ☒ AND, ensure that:

- a) any such disclosure is made in compliance with section 8 of the *Privacy Act*, which allows disclosures of personal information with consent of the individual to whom the information relates (subsection 8(1)) or without consent in certain and limited circumstances pursuant to subsection 8(2) of the Act;
- b) only personal information elements that are necessary for the intended purpose are disclosed;
- c) the organization or third party receiving the personal information is authorized to do so;
- d) administrative, physical and technical safeguards appropriate to the sensitivity of the information will be applied to protect the information during and after its transmission (see Question 15);
- e) the organization or third party to which the personal information will be disclosed for the administration of the program or activity are identified in the "Consistent Use" section in the relevant **PIB** in *CBSA Info Source*, including the specific purpose of the disclosure; the "**Privacy Notice**" or "**Consent Statement**" describes any disclosures of information; (For a copy of the CBSA Privacy Notice and Consent Statement template, contact the ATI and Privacy Division) and,
- f) the "Data Flow Diagram" or "Data Flow Tables" completed in "*Section 4 – Flow of Personal Information*" of the CBSA PIA include details on the disclosed personal information: (See Section IV of Appendix "C" of *Directive on Privacy Impact Assessment* for a list of elements that must be included in the data flow diagram or data flow tables.)

10.3 ☒ AND, any disclosure of personal information to another federal institution or outside the Government of Canada is governed by a formal agreement or arrangement (e.g., a Memorandum of Understanding, an accord, a contractual arrangement, etc.) to ensure that appropriate privacy protection clauses are included, and, where applicable, include provisions for inter-jurisdictional or transborder flows of personal information. Such clauses must cover the following topics:

- a) Control over personal information, where appropriate.
- b) Limitations on the collection, retention, use and disclosure of personal information.
- c) Measures (administrative, technical and physical) to protect the integrity and confidentiality of personal information.
- d) Measures governing the disposition of the personal information, where relevant
- e) Measures to ensure or verify that the personal information is only used for the purposes related to the agreement, arrangement or contract.

f) Obligations are to be extended to other parties such as subcontractors.

→ Continue to Question 11

NO

10.4 ☐ There is no disclosure of personal information within or outside the institution for purposes that are directly related to the administration of the program or activity.

→ Continue to Question 11

11. Accounting For New Uses or Disclosures Not Reported in CBSA Info Source

Will controls and procedures be implemented to account for any new use or disclosure of the personal information that is not included in the relevant PIB published in CBSA Info Source?

Statutory reference: Sections 7 to 11 of Privacy Act and section 4 of Privacy Regulations

Policy reference: Sections 6.1.9 and 6.2.2 of Directive on Privacy Practices

YES

11.1 ☒ Appropriate controls and procedures have been or will be implemented to ensure that:

- a) the head of the institution (The ATI and Privacy Director) or the appropriate delegate is notified about any new use or disclosure of personal information that is not reflected in the PIB description published in *CBSA Info Source*;
- b) the consent of the individual to whom the information relates is obtained in writing, as appropriate, prior to any new use of the information for an administrative purpose that is not reflected in the relevant PIB published in *CBSA Info Source*, unless the new use is considered to be consistent with the purpose for which the personal information was obtained or compiled and the Privacy Commissioner is notified, by the CBSA ATI and Privacy Director, forthwith regarding the new consistent use;
- c) except as permitted under subsection 8(2) of the *Privacy Act*, any disclosure of personal information for a purpose that is not reflected in the relevant PIB published in *CBSA Info Source* will only be made with the consent of the individual to whom the information relates;
- d) a record is kept for any new use or disclosure of personal information not described in the relevant PIB published in *CBSA Info Source*, and that this record is stored with the personal information to which it relates and retained for a minimum period of two years following such a use or disclosure; *(The record of use or disclosure should include the name and title of the person authorizing the use or disclosure; the name of the institution, person, organization or body receiving the information; a description of the use or purpose of disclosure; a copy of the information disclosed, or a description in sufficient detail to allow a determination of exactly what information was used or disclosed.)*
- e) if the information is disclosed to a federal investigative body under paragraph 8(2)(e) of the *Privacy Act*, the record of disclosure will be kept in a separate PIB for a period of two years where it will be available to the Privacy Commissioner for review upon request; *(e.g., Standard PIB "Disclosure to Investigative Bodies" PSE 913)*
- f) the Privacy Commissioner is notified, by the CBSA ATI and Privacy Director, forthwith, as required under subsection 9(4) of the Act, of any new use or disclosure that is consistent with the purpose

Name of Program / Activity / Service

PIA

for which the information was obtained or compiled, but which is not reflected in the relevant **PIB** published in *CBSA Info Source*;

- g) the relevant **PIB** is amended in time for the next edition of *CBSA Info Source* to include any new use(s) or disclosure(s) that are consistent with the purpose for which the information was obtained or compiled, as well as any routine use(s) or disclosure(s) that do not fall within the categories of purpose of collection or consistent use (e.g., these would include disclosures of the information under subsection 8(2) of the Act that take place on a regular basis. By including these routine uses or disclosures in the PIB, the CBSA would be relieved from the obligation to record each use or disclosure on the individual's file); and
- h) the Privacy Commissioner is notified, by the ATI and Privacy Director, prior to or forthwith, as required under subsection 8(5) of the Act, about any disclosures made or to be made in the public interest or in the interest of the individual to whom the information relates.
- i) Other

Detail : CBSA policy requires that any new use or disclosure of the personal information that is not included in the relevant PIB published in CBSA Info Source be identified to the ATIP Coordinator, who will notify the Office of the Privacy Commissioner and update the program PIB as required.

→ Continue to Question 12

****Ensure to provide the "controls and procedures" as an annex to this PIA****

NO

- 11.2 ☐ Please explain why such controls and procedures will not be implemented

Detail: *Provide adequate justification.*

→ Continue to Question 12

12. Safeguards - Statement Of Sensitivity

Has a Statement of Sensitivity (SoS) or similar analysis been completed to assess the degree of sensitivity of the personal information to be collected and retained for the program or activity? (Input to this section should be coordinated with and reviewed by the CBSA – IT - Security Directorate)

Statutory reference: Sections 7 and 8 of *Privacy Act*.

Policy reference: Appendix C of *Directive on Privacy Impact Assessment* and sections 6.2.17 to 6.2.21 of *Directive on Privacy Practices*, *Policy on Government Security*, *Operational Security Standard: Management of Information Technology Security (MITS)*

YES

- 12.1 ☒ The information contained in the SoS or similar analysis has been taken into account when assessing the level of risks to privacy in "Section 2 - Risk Area Identification and Categorization" of the CBSA PIA.

→ Continue to Question 13

Name of Program / Activity / Service

PIA

****Ensure to provide the "SOS" as an annex to this PIA****

NO

- 12.2 ☐ Please explain why a SoS or similar analysis was not considered necessary to assess the sensitivity of the information.

Detail: *(This information is mandatory)*

→ Continue to Question 13

13. Safeguards - Threat and Risk Assessment

Has a Threat and Risk Assessment (TRA) or a similar security assessment been completed for the program or activity? *(Input to this section must be coordinated with and reviewed by CBSA – IT - Security Directorate)*

Statutory reference: Sections 7 and 8 of *Privacy Act*.

Policy reference: Appendix C of *Directive on Privacy Impact Assessment* and sections 6.2.17 to 6.2.21 of *Directive on Privacy Practices, Policy on Government Security, Operational Security Standard: Management of Information Technology Security (MITS)*

YES

- 13.1 ☐ Reference the title of the TRA or other security assessment in "Section 6 – Supplementary Documents List" and provide a brief synopsis of the assessment in the space below:

Detail: *(This information is mandatory)*

- 13.2 ☐ AND, obtain assurances from the officials responsible for the program or activity that the measures recommended in the assessment have been implemented to ensure the confidentiality, availability and integrity of the personal information.

- 13.3 ☐ AND, ensure that any residual risks to personal information are known and accepted by the executive or senior official responsible for the program or activity and the Head or delegated authority for the *Privacy Act*. (ATI and Privacy Director)

→ Continue to Question 14

NO

- 13.4 ☒ If a TRA or similar security assessment is underway, simply reference that fact in the space below and indicate when it is likely to be completed. If there is no intent to complete one, please explain.

Detail: *Submissions collected as a result of the application for relief are not saved in electronic systems.*

→ Continue to Question 14

14. Safeguards - Administrative, Physical and Technical

Please identify below any administrative, physical and technical safeguards in place, or to be implemented, for this program or activity to ensure the confidentiality, availability and integrity of the personal

information. (Safeguards must be commensurate with the sensitivity of the information, the risks identified, and the nature of the media in which the information is stored, handled and transmitted. This section must be completed with input from CBSA – IT - Security Directorate)

Statutory reference: Sections 7 and 8 of Privacy Act

Policy reference: Appendix C of Directive on Privacy Impact Assessment and sections 6.2.17 to 6.2.21 of Directive on Privacy Practices, Policy on Government Security, Operational Security Standard: Management of Information Technology Security (MITS)

Please check all that apply, including safeguards identified by the TRA or similar security assessment.

14.1 Administrative safeguards

- ☒ Internal security and privacy policies and procedures
- ☒ Staff training on privacy and the protection of personal information
- ☒ Screening and security checks of employees
- ☒ Appropriate security levels for employees who will have access to personal information
- ☒ Contingency plans and documented procedures in place to identify and respond to security and privacy breaches, and to communicate security violations to the data subject, law enforcement authorities and relevant program managers
- ☐ Regular monitoring of users' security practices
- ☒ Methods to ensure that only authorized personnel who need to know have access to personal information
- ☐ Other

Detail: (This information is mandatory)

14.2 Physical safeguards

- ☒ Restricted access areas
- ☒ Security guards
- ☒ Identification badges are worn by staff at all times
- ☒ After hours alarms and monitoring systems
- ☒ Locked filing cabinets
- ☒ Combination locks
- ☒ Safes
- ☐ Cipher locks
- ☒ Key cards
- ☐ Video surveillance (closed-circuit television)
- ☒ Secured server locations
- ☒ Backups secured off-site
- ☐ Other

Detail: (This information is mandatory)

Name of Program / Activity / Service

PIA

14.3 Technical safeguards

- ☒ Role-based user authorization and authentication
- ☐ Biometrics
- ☒ Passwords (minimum of 6 characters long, include alpha and numeric characters)
- ☒ Passwords are changed by users every 90 days and recently used passwords cannot be re-used)
- ☒ Password protected screensavers
- ☒ Session-time out security (automatically locks an account after a session has been idle for a specified amount of time)
- ☒ Firewalls
- ☒ Intrusion Detection System (IDS)
- ☒ Virtual Private Network (VPN)
- ☒ Encryption of sensitive information
- ☒ Government of Canada Public Key Infrastructure Certificates (PKI)
- ☐ External Certificate Authority (CA)
- ☐ Audit trails
- ☐ Other

Detail: (This information is mandatory)

→ Continue to Question 15

****Ensure to provide the "controls and procedures" as an annex to this PIA****

15. Technology and Privacy - Tracking Technologies

Will the information system(s) used to deliver the program or activity employ cookies or other tracking technologies to collect personal information about users and their transactions? (Input to this section should be coordinated with and reviewed by the CBSA – IT - Security Directorate)

Statutory reference: Sections 4 to 10 of the Privacy Act and section 4 of Privacy Regulations

Policy reference: Subsections 6.1.1, 6.1.3, 6.1.9, 6.2.9 to 6.2.13, 6.2.17 and 6.2.23 of Directive on Privacy Practices

YES

- 15.1 ☐ The specific tracking technologies to be used is adequately described under Part 6: Technology and Privacy of "Section 2 – Risk Area Identification and Categorization" of the CBSA PIA; (For example, the use of an audit trail that records information, such as user logon ID, date and time of logon, logout, user location, terminal identity, name and ID of client records accessed, including edits or changes made during each user session, etc. The information is used to verify that only authorized users access personal information and to ensure that access can be linked to specific individuals to support the investigation of suspected or alleged misuse. The information is retained for a period of two years.)

- 15.2 ☐ AND, the collection of any personal information using such technologies is reflected in the relevant PIB and in "Section 3 – Analysis of Personal Information Elements" of the CBSA PIA;

Name of Program / Activity / Service

PIA

- 15.3 ☐ AND, the use of such technologies to collect information about users and their transactions is adequately reflected in the "Privacy Notice";
- 15.4 ☐ AND, those responsible for implementing and using tracking technologies to collect personal information or who may have access to personal information collected through these methods are made aware of privacy and security policy requirements;
- 15.5 ☐ AND, where personal information collected through such tracking technologies is used to make a decision that directly affects the individual to whom the information relates, it will be retained for a minimum of two years after the last administrative action as required under the *Privacy Regulations*.
 → Continue to Question 16

NO

- 15.6 ☒ Tracking technologies are not used to collect personal information about users.
 → Continue to Question 16

16. Technology and Privacy - Surveillance or Monitoring

Will the new or modified program or activity result in new or increased surveillance or monitoring of a targeted population? (Input to this section should be coordinated with and reviewed by the CBSA – IT - Security Directorate)

Statutory reference: Sections 4 to 10 of *Privacy Act*, section 4 of *Privacy Regulations* and section 8 of the *Charter of Rights and Freedoms*
Policy reference: Subsections 6.1.1, 6.1.9, 6.2.9 to 6.2.13 and 6.2.17 of *Directive on Privacy Practices*

YES

- 16.1 ☐ Consult with your legal advisors to determine whether or not such surveillance or monitoring activities raise any issues relating to the *Charter of Rights and Freedoms*, the *Privacy Act* or other applicable acts.
- 16.2 ☐ And, ensure the surveillance or monitoring method(s) to be used, the characteristic(s) of the targeted population and the scope of the surveillance or monitoring are adequately described under Part 6: Technology and Privacy of "Section 2 – Risk Area Identification and Categorization" of the CBSA PIA.
- 16.3 ☐ AND, any personal information collected or created as a result of such surveillance or monitoring is described in the relevant **PIB** and in Section 3 – Analysis of Personal Information Elements" of the CBSA PIA.
- 16.4 ☐ AND, the collection or use of personal information through surveillance or monitoring is adequately reflected in the "Privacy Notice", unless such notification might result in the collection of inaccurate information or defeat the purpose or prejudice the use for which the personal information is collected.
☐ If notice about surveillance or monitoring will not be provided

Detail explain why: (This information is mandatory)

- 16.5 ☐ AND, those responsible for implementing and using such surveillance or monitoring method(s) or who may have access to personal information collected or created through these methods are made

Name of Program / Activity / Service

PIA

aware of privacy and security policy requirements.

→ Continue to Question 17

NO

16.6 ☒ The new or modified program or activity will not result in surveillance or monitoring.

→ Continue to Question 17

17. Considerations Related to Compliance, Regulatory Investigation, Enforcement

Does the program or activity involve compliance/regulatory investigation or law enforcement, surveillance or intelligence gathering that targets specific individuals against whom penalties, criminal charges or sanctions may be applicable?

Statutory reference: Sections 4 to 10 of *Privacy Act*, section 4 of *Privacy Regulations* and section 8 of the *Charter of Rights and Freedoms*

Policy reference: Subsections 6.1.1, 6.1.9, 6.2.9 to 6.2.13 and 6.2.17 of *Directive on Privacy Practices*

YES

17.1 ☒ Consult with your legal advisors to determine whether or not the compliance/regulatory investigation or law enforcement activities raise any issues relating to the *Charter of Rights and Freedoms*, the *Privacy Act* or other applicable acts.

17.2 ☒ AND, identify the legislative authority and the specific regulatory or law enforcement purpose involved:

Detail: Information provided by a person in support of an application for Ministerial relief is collected under the authority of subsection 15(1) of the IRPA. Drafting a recommendation for the Minister of Public Safety and Emergency Preparedness requires assessing the applicant's submissions within a context of the immigration information in the possession of both IRCC and the CBSA. As part of this analysis, the MRU may identify cases in which applicants may have provided information contradictory to what had been previously provided in the context of advancing other applications. Where an MRU analyst believes such contradictions might rise to the level of misrepresentation, the inconsistencies may be brought to the attention of CBSA or IRCC enforcement officers to determine whether any proceedings relating to misrepresentation, or the vacation of refugee protection status, are warranted.

17.3 ☐ AND, if the legislative authority differs from the legal authority for the program or activity, ensure it is adequately reflected in the response to Question 1 of "Section 5 – Privacy Compliance Analysis" and in "Section 1 – Overview and PIA Initiation" of the CBSA PIA.

17.4 ☒ AND, any personal information collected or created as a result of such regulatory or criminal enforcement, surveillance or intelligence gathering program or activity is described in the relevant **PIB** and in "Section 3 – Analysis of Personal Information Elements" of the CBSA PIA.

17.5 ☒ AND, the collection or use of personal information through these compliance / regulatory investigation or enforcement activities is adequately reflected in the "Privacy Notice", unless such notification might result in the collection of inaccurate information or defeat the purpose, or prejudice the use, for which the personal information is collected.

☐ If notice about the compliance/regulatory investigation or law enforcement activities will not be provided.

Name of Program / Activity / Service

PIA

Details explain why: *(This information is mandatory)*

NO

- 17.6 ☐ The program or activity does not involve the conduct of regulatory or criminal enforcement, surveillance or intelligence gathering.

SECTION 6 - Summary of Analysis and Recommendations

The ATI and Privacy Division will document the recommendations resulting from the risk identification and categorization, as well as in a manner that is commensurate with the risk identified. The risks and recommendations will be incorporated into the action plan as described in Annex B: Office of the Privacy Commissioner Expectations (2011)

Risk One - Over-Collection of Information:

With the Ministerial relief program, there is risk of the over-collection of information, as applicants may choose to provide information that has not been requested or required by the CBSA. Because an applicant may not know which elements of their particular circumstances the Minister of Public Safety ("the Minister") may find compelling, and given that "national interest" is not a legally-defined or static concept, there is a tendency for applicants to submit a broad range and high volume of material. By the nature of the "legal test" applicable to Ministerial relief assessments (the onus is on the applicant to satisfy the Minister and not the contrary), applicants are not precluded from providing any information they may wish with the goal of satisfying the Minister that granting relief would not be contrary to the national interest. An example of this is the applicant's Social Insurance Number. Despite the CBSA not requiring this information, applicants often choose to submit documents which contain it.

Mitigation:

The over-collection of information will always be a risk that requires managing. Due to the "legal test" applicable to MR assessments, it is not possible to develop a comprehensive list or other similar limitation on the type of information that an applicant may provide toward their application.

However, the MR form may help streamline future applicant submissions by means of standardizing certain information required or recommended to be provided to the CBSA at the outset – though an applicant may still choose to provide any additional information or documentation for the Minister to consider at any time. Administrative law requires that all submissions made by an applicant be put before the decision maker for consideration, regardless of the degree of their relevance to the national interest assessment. Furthermore, as MR decisions are subject to judicial review, the complete submissions of an applicant need to be included as part of the certified tribunal record in the event that the applicant litigates the MR decision.

Risk Two – Unauthorized Exposure or Loss of Information Collected:

MR applicants submit hard copies of their submissions and physical files are held by the MR unit. With physical files there is the risk that sensitive information is left out in the open, or could potentially be misplaced. Additionally, due to the approval process that MR files are subject to, many employees at different offices within the CBSA may come into contact or have access to case-related information. MR applicants also provide information and submissions to, and correspond with, the MR unit by email.

Mitigation:

In order to mitigate such risks, the MR unit has filing cabinets secured by combination locks. MR unit employees are also provided with security awareness training at regular intervals and are aware of security and privacy policies and procedures. This training also applies to all employees who would come into contact with MR application packages and decisions through the approvals process: Director's Office, Director General's Office, Vice-President's Office, President's Office and the Minister's Office.

Any electronic records or personal information of the applicants are kept within the CBSA's secure network or accessed via the CBSA's secure network. In the event a computer is left unattended with sensitive information on the screen and/or readily accessible, the computer will time out and lock, requiring a password to re-enter. Additionally, all computers are housed on a secure floor requiring a key card to enter.

The CBSA is transitioning to Apollo, an Agency-specific form of the new Government of Canada electronic document and records management system called GCDOCS, which will replace personal and shared drives and email archives by a single corporate document repository. Apollo allows the safeguarding of information by restricting access and designating permissions to individual folders, and the electronic holdings of the MR Unit will be very strictly controlled. In addition, all staff must complete mandatory biennial information security training. The transfer of client records held in email archives has already begun and it is a program priority to complete the full transfer within the 2017-2018 fiscal year.

SECTION 7 - SUPPLEMENTARY DOCUMENTS LIST

List all supplementary documents that support the conclusions of this CBSA Privacy Impact Assessment. For each document, cite the specific sections of the documents (subject, chapter, page, paragraph, etc.) that correspond with the CBSA PIA and link them to the PIA sections.

Document	Document Ref.	PIA Ref.
1. Statement of Sensitivity	Entire document	Section 5.12
2. Application for Declaration of Relief Under Subsection 42.1(1) of the IRPA (BSF 766E)	Entire document	Section 3
3. Privacy / Consent Statement for form BSF 766E	Entire document	Sections 5.5, 5.8
4. Amended Regulations, Ministerial Relief Program	Entire document	Sections 1.10, 5.1

Additional documents used or related to the CBSA PIA may include:

- Project and Product Scope
- Business Case / Project Charter
- Business Requirements
- Threat Risk Assessments
- Risk Management Plan
- Contracts / Memoranda of Understanding / Agreements

Name of Program / Activity / Service

PIA

SECTION 8 - FORMAL APPROVAL

The following signature represents a commitment to comply with sections 4 to 8 of the *Privacy Act* and the related privacy policy requirements outlined in the CBSA PIA as they relate to the administration of the identified program or activity.



Signature of CBSA Vice President lead for program or activity

7/3/17

Date

Note: Responsibility for sections 4 to 8 of the *Privacy Act* rests with all employees of government institutions that handle personal information. Officials who manage such programs and activities are responsible for ensuring that such requirements are implemented as part of the administration of the program or activity.

The following signature represents a commitment by the Head of the institution or his/her delegate(s) who is responsible for establishing personal information banks in accordance with section 10 of the *Privacy Act*.



Signature of CBSA ATI and Privacy Director

MAR 03 2017

Date

Note: Under the *Privacy Act*, the Head or his/her delegate(s) is responsible for complying with legal and relevant privacy policy requirements related to the approval and registration of personal information banks

Name of Program / Activity / Service

PIA

Annex A: Privacy Compliance Checklist and Other Considerations

Note: The table below must be used to keep an account of actions completed and to track outstanding actions required to achieve privacy compliance:

Privacy Compliance Analysis question #	Action required to support legal and policy compliance (cross reference to relevant question of <i>Section 5 – Privacy Compliance Analysis</i>)	Done	To be done
1	Legal authority for the program or activity has been established and is reflected in the relevant PIB.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2	a) The categories and elements of personal information to be collected for the new program or activity have been carefully assessed based, for example, on the CBSA's experience gained with the administration of a similar program or activity. The personal data collected will be limited to only that which is required.)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	b) Categories and elements of personal information have been described in the relevant PIB for the program or activity.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	c) Controls and procedures will be implemented to ensure the CBSA does not collect more personal information than necessary for the program or activity and that a continuing need exists for the personal information and its collection.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
4 and 5	a) All of the requisite "Privacy Notices" and "Consent Statements" that meet the requirements of sections 6.2.9 to 6.2.12 of the <i>Directive on Privacy Practices</i> have been drafted. (Texts of the notices and consent statements must be included as an annex.) For a copy of the CBSA Privacy Notice and Consent Statement template, contact the ATI and Privacy Division.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	b) Controls and procedures have been implemented to keep records of individual consents, and to ensure that persons acting on behalf of individuals who do not have the capacity to provide consent have the authority to do so under section 10 of the <i>Privacy Regulations</i> .	<input checked="" type="checkbox"/>	<input type="checkbox"/>
7	a) A Records Disposal Authority (RDA) has been approved by Library and Archives Canada to authorize the disposal of the records containing personal information for the program.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	b) Controls and procedures have been implemented within the program or activity and the CBSA ATI and Privacy Division to ensure that information that has been used for an administrative purpose will be kept for the minimum retention period established by the Privacy Regulations.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	c) Reference to the RDA, the retention period and the disposition standards for the program have been cited in the relevant PIB.	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Name of Program / Activity / Service		PIA	
Privacy Compliance Analysis question #	Action required to support legal and policy compliance (cross reference to relevant question of <i>Section 5 – Privacy Compliance Analysis</i>)	Done	To be done
8	Controls and procedures are in the process of being implemented to ensure that the personal information associated with the program is as accurate, complete and up-to-date as necessary.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Other Privacy Considerations related to specific principles that are not explored in the previous 17 sections: (these considerations should be explored in the Executive Summary)			
Openness	Describe how the results of any privacy impact assessment or audit will be made available to the public. The Executive Summary will be published on the external CBSA ATI and Privacy Division website at http://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/pia-efvp/atip-aiprp/pias-sefp-eng.html	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Are policies and practices relating to the proposal's management and handling of personal information available to the public?	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Is there a communications plan to explain to the public how personal information will be managed and protected?	<input type="checkbox"/>	<input checked="" type="checkbox"/>
	Is there a clearly defined and easy process for individuals to access such information and/or communicate with appropriate individuals with respect to policies and practices relating to management and protection of personal information?	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Where appropriate, will public consultation take place on the privacy implications of the proposal?	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Individual's Access to Personal Information	Is the system designed to ensure that an individual can have access to his/her personal information, including all other programs or applications that have received copies of the information? s. 12(1)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Are there documented procedures developed or planned on how to make privacy requests or requests for the correction of personal information? s. 12 (2)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Are individuals provided with access to their personal information in the official language of their choice? s. 17(2)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	If appropriate, are individuals provided with access to their personal information in an alternative format? s. 17(3)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Challenging	Are the complaint procedures for the proposed program or service	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Name of Program / Activity / Service		PIA	
Privacy Compliance Analysis question #	Action required to support legal and policy compliance (cross reference to relevant question of <i>Section 5 – Privacy Compliance Analysis</i>)	Done	To be done
Compliance	consistent with legislated requirements? s. 29-35		
	To improve information management practices and standards, has a procedure been established to log and periodically review the nature, frequency and resolution of complaints?	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Are there oversight and review mechanisms implemented or available to ensure accountability?	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Have oversight agencies, including the Office of the Privacy Commissioner, issued reports or opinions on issues that would be relevant to the proposal?	<input type="checkbox"/>	<input checked="" type="checkbox"/>

Annex B: Office of the Privacy Commissioner Expectations

In their March 2011 document, *Expectations: A Guide for Submitting Privacy Impact Assessments to the Office of the Privacy Commissioner of Canada*, the Office of the Privacy Commissioner (OPC) has expressed the importance of analysing the risks of the project, program or initiative against the ten universal privacy and fair information practice principles of the Canadian Standards Association Model Code for the Protection of Personal Information.

The most relevant demonstration of the privacy risk and compliance analysis is the action plan. The OPC has said the following in their **Expectations** guide with respect to the action plan:

Once privacy risks and their proposed mitigating measures have been identified, we expect to see an Action Plan drawn up by the institution, indicating a specific time frame for remedying or mitigating the risks that have been identified, and if possible, naming a specific person or staff position accountable for taking action.

The action plan must list all privacy risks and compliance issues identified in the PIA and supplementary documentation. All risks and issues must be organized by the 10 universal privacy principles.

All recommendations and proposed mitigation strategies must also be described in the action plan. Identify the responsible program area and the timeline for completion or implementation of the strategy. The ATI and Privacy Division will provide programs with an action plan template to be addressed near the end of the PIA process.

The expectations of the OPC for each privacy principles are included below for your reference.

Accountability

Under this principle the OPC would expect to see documentation of an administrative structure for privacy, including input from legal services, access to information and privacy and information technology branches within an institution, with defined processes for determining when new projects require PIAs, for carrying them out, implementing mitigating measures and auditing for assurance of compliance. We expect PIA reports to be signed off at the appropriate level, and that training in privacy issues and procedures has been documented and is refreshed with employees regularly; and that privacy protective language is included in all contracts with third parties handling personal information in accordance with TBS guidance documents and internationally accepted best practices; and that regularly scheduled privacy compliance audits will be undertaken and the findings acted upon.

Identifying Purposes

The Privacy Act restricts federal government institutions to the collection of personal information that relates directly to an operating program or activity of the institution, so we would expect to see a clear description of the program and why each piece of information is needed; a description of the legislative authority for the collection; a clear listing of all the data elements collected; copies of any relevant documents such as application forms identifying the purpose for the collection or on-line notices of use; a copy of an up to date Personal Information Bank (PIB) description; a statement of any proposed new consistent use of information previously collected and a clear rationale as to how the use is reasonable

and directly connected to the original collection -- this may include an analysis of how an individual to whom it relates would reasonably expect it to be used for that purpose; a statement outlining any intended secondary uses of the information; whether the information is collected directly from the individual and if not, why; and a description of how personal information used for planning, forecasting or statistical purposes would be anonymized or de-linked from individual identifying information.

Consent

This is closely tied to the Identifying Purpose principle. Under this principle, OPC would expect to see a copy of notification language on forms or websites; a clear description of the purpose for collection; a rationale for not seeking consent, as is provided for in the Privacy Act; for web sites, a copy of the Privacy Notice Statement under which personal information is submitted to the institution.

Limiting Collection

Under this principle, OPC would expect to see a clear justification of the need for each data element collected, in keeping with the requirement of the Privacy Act that no personal information is to be collected by a government institution unless it relates directly to an operating program or activity of the institution; an indication that a data minimization exercise has been undertaken to ensure that each data element is necessary and that this exercise will be refreshed regularly; and that information collected from another department for a secondary use will be purged of all but the essential data elements before use.

Limiting Use, Disclosure and Retention

Under this principle, OPC would expect to see a description of the specific uses and proposed disclosures of the information; a clear statement limiting the use of the information to the purposes identified; a clear retention policy and disposition schedule that is also noted in the PIB; a process for destruction of the information that is in keeping with the Privacy Act and Regulations; copies of MOUs or agreements with third parties to whom information is disclosed governing its use, retention and disclosure, and clauses with contractors or sub-processors of information indicating the originating institution has the right to audit for compliance with privacy provisions.

Accuracy

Under this principle, OPC would expect to see a description of the process used by entities to ensure accuracy, particularly when administrative decisions are made; a description of how changes to records are logged and monitored; a statement of whether automated decision-making based on risk profiles is being undertaken and how automated decisions are vetted for accuracy; an explanation of the processes open to individuals seeking to correct information; a description of the process by which second or third parties to whom information has been disclosed will be notified of changes and corrections to the record; and a description of how audit trails of records transactions are monitored and evaluated.

Safeguards

OPC would expect to see under this principle a description of the physical and electronic safeguards that are in place to protect information; a Threat & Risk Assessment (TRA) with emphasis on privacy risks and concerns and a discussion of how these concerns have been remedied or addressed; a notation that encryption is used for personal information both in transit and at rest; a description of how system logs of information transactions are monitored for inappropriate use, including viewing of the information; strong electronic access control, including controls on remote access, and the use of mobile devices;

policies for the use of portable storage devices such as flash drives; a description of role-based access controls; and a description of the steps taken to ensure complete destruction of the information at the end of its life cycle.

Openness

Under this principle, OPC would expect to see a summary of the PIA written in plain, understandable language, posted on the institutional website in a manner accessible to the general public and containing a link to the relevant PIB description in CBSA Info Source; for particularly sensitive or privacy invasive programs we would expect to see the public communications plan described in the PIA, including a variety of methods such as posters, brochures and media announcements as well as detailed discussion of the PIA in the institution's Annual Report under the Privacy Act; a description of consultations with key stakeholders and the privacy risks or concerns raised should be readily available on the website; the name and contact information of an individual accountable for the handling of personal information should be easily obtained through the website or by calling the institution's main public number.

Individual Access

Under this principle, OPC would expect the PIA to include a description of any informal process the CBSA may have in place for access to and correction of personal information; an up to date and comprehensive description of information contained in the PIB corresponding to the initiative; a description of the process by which information in the hands of third parties is corrected following requests; a description of how the general public is made aware of these processes, for example, by a link and/or a toll-free number shown on the home page of the institutional website.

Challenging Compliance

OPC would expect to see the PIA address this principle by indicating clearly who is responsible for receiving and resolving privacy complaints; describing complaints that may have been received in any similar activity or pilot project and how they were handled; including privacy issues in project evaluations or feasibility reports; describing how and when compliance audits for privacy will be undertaken; including information on how to file a complaint with OPC under the Privacy Act; and reporting in some detail on specific and/or systemic privacy issues in its Annual Reports.

Annex C: Categories of Personal Information

The **Description** section in a personal information bank (PIB) describes the personal information in the records to which the bank relates. Treasury Board Secretariat has established the following categories of personal information, which give examples of specific elements of personal information that fall under each category. The purpose of the categories is to reduce the number of personal information elements that need to be listed in the Description section. These categories are representative of the personal information collected by most institutions, and they now appear in many of the CBSA registered PIBs. The ATI and Privacy Division modified the original list to reflect CBSA business lines.

Biographical information (e.g. work history, curriculum vitae, family information, Passenger Information, etc.)
 Biometric information (e.g. blood type, eye or facial scan, DNA, finger / hand prints, etc.)
 Contact information (e.g. work and / or home information, including postal and e-mail addresses, telephone, fax, cell phone numbers, etc.)
 Citizenship status or Nationality (e.g. citizen, landed immigrant, etc.)
 Crew detailed information
 Criminal checks / history (e.g. information related to criminal record checks, investigations, charges, conviction dates and locations, pardons, etc.)
 Date of birth
 Date of death
 Destination City
 Employee identification number (e.g. Personal Record Identifier)
 Employee personnel information (e.g. records of attendance and leave, notices of disciplinary action, alternative work arrangements, decisions concerning compensation and fitness for work, official languages qualifications, salary, deductions, level of security clearance, performance reviews and appraisals, rating board assessments, including evaluation notes from staffing boards, training and development course applications and evaluations, etc.)
 E-Ticket Information
 Financial information (e.g. income, investments, mortgages, loans, orders of garnishment, financial institution information for direct deposit and other banking purposes, including name and branch number of institution, account number(s) and name(s) on accounts, etc.)
 FOSS Case Number
 Gender
 Itinerary Cities
 Language (e.g. mother tongue, official and other languages, etc.)
 Medical information (e.g. psychological assessments, blood type, etc.)
 Name (e.g. last name (surname/family name), given names (first, second or more), maiden name, nicknames, aliases, etc.)
 Opinion or views of, or about, individuals
 Passenger Name
 Passport Number or Travel Document Number
 Place of ticket purchase

Name of Program / Activity / Service

PIA

Photos

Physical attributes (e.g. height, weight, color of hair and eyes, physical markings (scars, tattoos, body piercing), etc.)

Place of birth

Place of death

Port of Embarkation and Port of Debarkation

Signature

Special Travelling Considerations such as Employee Pass, Buddy Pass and Parental Passes

Visa Number



Scenario-Based Targeting for High-Risk Travellers

Privacy Impact Assessment

Business Intelligence and Risk Assessment Division
October 18, 2013 / Ver. 14

Protected B

Version Control

Version	Author	Action	Date
1.0	Oliver Javanpour	Template clean up and format for use	Oct 20, 2012
1.a		Introduction	Nov 15, 2012
1.b		Core PIA	Dec 10, 2012
1.c		Overview & dataflow	Jan 02, 2013
1.d	Doris Beck	Review and comments	Jan 16, 2013
2.0	Oliver Javanpour	Major revision and update Overview and preamble sections	Jan 20, 2013
2.a		Questionnaire	Feb 01, 2013
2.b	Oliver Javanpour	Review with Doris Beck	Feb 06, 2013
2.c	Doris Beck	Review and edit	Feb 12, 2013
2.d	Oliver Javanpour	Risk and mitigation	Feb 12, 2013
3.0	Oliver Javanpour	Finalized first draft	Feb 20, 2013
4.0	Andre Hiotis	Conversion to CBSA template and re-write of section 1, 4, and 5.	April 8, 2013
5.0	Andre Hiotis	Update based on comments from Diana	April 13, 2013
6.0	Andre Hiotis	Update based on comments from Doris and Diana	April 19, 2013
7.0	Scott Crosby	Update based on comments from Doris, Andre and Diana	May 10, 2013
8.0	Scott Crosby/Doris Beck	Update	May 13, 2013
9.0	Scott Crosby/Doris Beck	Update	May 17, 2013
10.0	Scott Crosby/Doris Beck	Update based on stakeholder comments	May 29, 2013
10.1	Scott Crosby/Doris Beck	Updates per stakeholder review meeting	May 29, 2013
10.2	Doris Beck	Stakeholder reviews accepted, with additional feedback	June 6, 2013
10.3	Doris Beck	Terrorism related crimes, etc incorporated into exec summary and type of personal info sections.	June 13, 2013
10.3a	Doris Beck	Section 6.3.3 amended	June 21, 2013
10.4	Scott Crosby/Doris Beck	Updates per recommendations from Legal Services and ATIP	July 15, 2013
10.4	Doris Beck	Suggested updates based on ATIP review (draft)	Aug 28/13
10.5	Doris Beck	Suggested updates for review with	Sept 3, 2013

		Scott	
10.5	DB	Reference to RCMP MOU	Sept 4, 2013
10.5	Scott Crosby	Blending revisions and making edits	Sept 6, 2013
10.5	Doris Beck	Formatting changes and confirmation of edits	Sept 9, 2013
10.6	Doris Beck	Updates based on internal review	Sept 12, 2013
11.0	Doris Beck	Final version to ATIP	Sept 17, 2013
12.0	Robin Lortie	Suggested updates based on ATIP review	Sept. 21, 2013
13.0	Doris Beck	Updates based on ATIP discussion	Sept. 30, 2013
14.0	Doris Beck	Executive Summary updated per ATIP recommendation. Dataflow diagram also updated.	Oct. 18, 2013

Change Control Table

Version	Date	Change Made By	Change Requested By	Change

Table of Contents

VERSION CONTROL	2
EXECUTIVE SUMMARY	7
ABBREVIATIONS AND ACRONYMS	9
DEFINITIONS	10
SECTION 1 - OVERVIEW AND INITIATION	12
SECTION 2 - RISK AREA IDENTIFICATION AND CATEGORIZATION	17
Type of Program or Activity	17
Type of Personal Information Involved and Context	19
Program or Activity Partners and Private Sector Involvement	19
Duration of the Program or Activity	20
Program Population	20
Technology and Privacy	20
Personal Information Transmission	21
Risk Impact to the CBSA	22
Risk Impact to the Individual or Employee	23
A) Beyond the Border Privacy Principles	24
SECTION 3 - ANALYSIS OF PERSONAL INFORMATION ELEMENTS	28
SECTION 4 - FLOW OF PERSONAL INFORMATION	34
4.1 Data Flow - Diagram	34
4.2 Work Flow - Diagram	35
Data Flow - Description	36
4.2 Data Flow Model - Table	38
4.3 Internal Use and Disclosure	41
4.4 External Use and Disclosure	41
4.5 Retention / Storage	41
4.6 Other Possible Considerations	41
SECTION 5 - PRIVACY COMPLIANCE ANALYSIS	42
1. Legal Authority For Collection Of Personal Information	42
2. Necessity To Collect Personal Information	45
3. Authority For the Collection, Use or Disclosure Of the Social Insurance Number ...	46
4. Direct Collection - Notification and Consent (as appropriate)	46
5. Indirect Collection - Consent or Authority Under Sec. 10 of Privacy Regulations	47
6. Indirect Collection - Without Notification and Consent	48
7. Retention and Disposal of Personal Information	49
8. Accuracy Of Personal Information	50
9. Use Of Personal Information	52
10. Disclosures Directly Related to the Administration of the Program or Activity	54
11. Accounting For New Uses or Disclosures Not Reported in CBSA Info Source	56
12. Safeguards - Statement Of Sensitivity	57

13. Safeguards - Threat and Risk Assessment	57
14. Safeguards - Administrative, Physical and Technical.....	58
15. Technology and Privacy - Tracking Technologies	60
16. Technology and Privacy - Surveillance or Monitoring	60
17. Considerations Related to Compliance, Regulatory Investigation, Enforcement ..	61
SECTION 6 - SUMMARY OF ANALYSIS AND RECOMMENDATIONS.....	63
SECTION 7 - SUPPLEMENTARY DOCUMENTS LIST [TBC]	64
SECTION 8 - FORMAL APPROVAL	66
ANNEX A: PRIVACY COMPLIANCE CHECKLIST AND OTHER CONSIDERATIONS.....	67
ANNEX B: OFFICE OF THE PRIVACY COMMISSIONER EXPECTATIONS	70
ANNEX C: CATEGORIES OF PERSONAL INFORMATION	73

Privacy Impact Assessment Date / Version:	2013-10-18 / Version 14.0
Office of the Privacy Commissioner file #:	
Project Implementation Plan (if applicable)	2014-01-28
Federal Institution:	Canada Border Services Agency (CBSA)
Related Class of Record Number:	CBSA IST 001
Personal Information Bank:	CBSA PPU 008
Government Official Responsible for PIA:	Vice President, Programs Branch
Delegate for section 10 of the <i>Privacy Act</i> :	ATI and Privacy Director

EXECUTIVE SUMMARY

Scenario Based Targeting

The Scenario-Based Targeting (SBT) initiative is aligned with the Canada Border Services Agency's (CBSA) border vision and the Government of Canada's commitments under the *Beyond the Border Action Plan* to address threats earlier to enhance our security and accelerate the flow of legitimate goods and people. This initiative is an important part of the Beyond the Border declaration, negotiated between Canada and the United States (US) in 2011, whereby Canada committed to implementing a harmonized methodology for the screening of all travellers.

The CCRA implemented the Advance Passenger Information (API)/Passenger Name Record (PNR) program in October 2002 mandating the collection of prescribed information from commercial air carriers to identify persons who are or who may be involved with terrorism or terrorism-related crimes or other serious crimes, including organized crime, that are transnational in nature. In 2003 and 2004, the CBSA established the High-Risk Traveller Identification Initiative (HRTI) jointly with the United States Customs and Border Protection (US CBP) to extend the API/PNR program to identify high-risk air travellers. Both parties agreed to implement a risk scoring methodology within their automated passenger systems to conduct risk assessment of unknown high-risk air passengers flying into their respective countries.

After an extensive analysis of the risk scoring methodology and the continued commitment to comply with agreements made with the US CBP, the CBSA undertook the replacement of risk scoring functionality with scenario-based rules functionality on a limited basis. In January 2010, the Executive Policy Committee approved the implementation of a long term solution for SBT within the Passenger Information System (PAXIS).

SBT-related enhancements to PAXIS will increase the efficiency, effectiveness and accuracy of the Targeting Officer's otherwise manual and labour-intensive work, and thereby help facilitate the more efficient movement of legitimate people while safeguarding the border and the security of Canada. The enhancements also dramatically reduce scenario deployment times and costs enabling the CBSA to respond to imminent threats.

The scope of the SBT project is to make changes to PAXIS, previously using a risk scoring methodology, to accommodate a scenario-based methodology to enhance the processes which identify suspected high-risk travellers in the air mode. SBT will more effectively direct the focus on a smaller segment of the travelling

population who represent a potential high risk.

The SBT project and methodology is subject to the *Customs Act*, sections 7.1, and 107.1, the *Immigration and Refugee Protection Act*, paragraph 148(1)(d) and 149, the *Immigration and Refugee Protection Regulations*, Section 269, and the *Passenger Information (Customs) Regulations*, *Protection of Passenger Information Regulations*.

The Pre-Border Programs Division of the CBSA is undertaking the replacement of risk scoring functionality with scenario-based rules functionality using API/PNR information that are processed and maintained in PAXIS. The scope of this Privacy Impact assessment (PIA) is limited to assessing privacy risks associated with the deployment of the SBT methodology.

This PIA is an appendix to the overarching API/PNR Program PIA along with the High-Risk Traveller Identification Initiative (HRTI) PIA.

This PIA Report identified one minor privacy risk related to the API/PNR Program Personal Information Bank (PIB) in the manner in which it currently reflects risk scoring, rather than SBT methodology and does not fully reflect statutory authorities for use of the personal information. This risk will be mitigated or eliminated when the API/PNR Program PIB will be updated for March 2014.

Right of Access

An individual may formally request access to their personal information, or access to corporate records related to or created by scenario based targeting, by contacting the Access to Information and Privacy Division. More information about this can be found at: <http://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/pia-efvp/atip-aiprp/menu-eng.html>.

Accountability

If an individual has concerns about the collection, use, disclosure or retention of their personal information, they may issue a complaint to CBSA Access to Information and Privacy Division. Complaints should be made in writing, and include the individual's name, contact information, and a brief description of their concerns. Contact information for the Access to Information and Privacy Division at the CBSA can be found at <http://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/pia-efvp/atip-aiprp/contact-eng.html>.

ABBREVIATIONS AND ACRONYMS

The following is a list of abbreviations and acronyms used in this report:

Abbreviation	Description
API	Advance Passenger Information
ATIP	Access to Information and Privacy Division
ARS	Airline Reservation System
CBSA	Canada Border Services Agency
CIC	Citizenship and Immigration Canada
CPIC	Canadian Police Information Centre
CRA	Canada Revenue Agency
DAS	Data Acquisition Solution
FOSS	Field Operations Support System
HRTI	High Risk Traveller Initiative
ICES	Integrated Customs Enforcement System
ICS	Integrated Customs System
ID	Identification
IMS	Intelligence Management System
Interpol	International Criminal Police Organization
IRPA	Immigration and Refugee Protection Act
MOU	Memorandum of Understanding
NTC	National Targeting Centre
OPC	Office of the Privacy Commissioner
PAXIS	Passenger Information System
PIA	Privacy Impact Assessment
PIB	Personal Information Bank
PNR	Passenger Name Record
RCMP	Royal Canadian Mounted Police
RFI	Request for Information
SBT	Scenario Based Targeting
TBS	Treasury Board Secretariat
TRA	Threat and Risk Assessment
US CBP	United States Customs and Border Protection
US	United States

DEFINITIONS

This section provides definitions of the terms frequently used in this report:

Terminology	Description
Action Plan	The Action Plan describes the steps that the Program will take to address privacy risks that have been identified by CBSA and the OPC.
Administrative purpose	The <i>Privacy Act</i> defines an “administrative purpose” to be the use of an individual’s personal information in a decision-making process that directly affects that individual.
Advanced Passenger Information (API)	<p>API includes:</p> <ul style="list-style-type: none"> • <i>surname, first name and initial or initials of any middle names;</i> • <i>date of birth</i> • <i>the country that issued them a passport or travel document or, if they do not have a passport or travel document, their citizenship or nationality;</i> • <i>their gender;</i> • <i>their passport number or, if they do not have a passport, the number on the travel document that identifies them; and</i> • <i>their reservation record locator or file number</i>
Confidentiality	The Policy on Government Security (2009) defines “confidentiality” to be the a characteristic applied to information to signify that it can only be disclosed to authorized individuals to prevent injury to national or other interests.
Consistent use	Is a use that has a reasonable and direct connection to the original purpose(s) for which the information was obtained or compiled. This means that the original purpose and the proposed purpose are so closely related that the individual would expect that the information would be used for the consistent purpose, even if the use is not spelled out.
Data Matching	A comparison of personal information obtained from a variety of sources, including personal information banks, for administrative or non-administrative purposes. Data matching is a specialized activity involving the collection, use and disclosure of personal information that is subject to the various requirements of the <i>Privacy Act</i> .
Info Source	A series of annual Treasury Board Secretariat publications in which government institutions are required to describe their institutions, program responsibilities and information holdings, including Personal Information Banks (PIBs) and classes of personal information. The descriptions are to contain sufficient clarity and detail to facilitate the exercise of the right of access under the <i>Privacy Act</i> . Data-matching activities, use of the Social Insurance Number (SIN) and all activities for which privacy impact assessments were conducted have to be cited in <i>Info Source</i> PIBs, as applicable. The <i>Info Source</i> publications also provide contact information for government institutions as well as summaries of court cases and statistics on access requests.
National Targeting Centre (NTC)	The NTC is responsible for ensuring national security by detecting and interdicting the movement of high-risk people and goods. It operates 24/7 and acts as a focal point between international, national and local law enforcement agencies to protect Canada from emerging threats.
Passenger Name Record (PNR)	<p>Information regarding a persons’ travel itinerary, contained within a commercial carrier’s reservation system, created once a person makes a reservation. It includes:</p> <ul style="list-style-type: none"> • Name • Any collected API

	<ul style="list-style-type: none"> • PNR record locator code • Date of intended travel • Date of reservation • Date of ticket issuance • Travel agencies • Travel agent • Contact telephone information • Billing address • All forms of payment information • Frequent Flyer Information • Ticketing Field Information • Ticket number • Split/divided PNR Information • Go show information (ticket purchase without a reservation) • No show information • All travel Itinerary Information • Standby Information • Other names on PNR • Check in Information • Bag tag numbers (Baggage information) • Seat information • Seat number • One way tickets
Personal Information	Information about an identifiable individual as defined in section 3 of the <i>Privacy Act</i> . This definition, although lengthy, is not exhaustive, as indicated by the introductory phrase, "including, without restricting the generality of the foregoing". Information that is not specifically mentioned in the list may still be included in the definition of personal information if it qualifies as "information about an identifiable individual".
Personal Information Bank (PIB)	A description of personal information that is organized and retrievable by a person's name or by an identifying number, symbol or other particular assigned only to that person. The personal information described in the personal information bank has been used, is being used, or is available for an administrative purpose and is under the control of a government institution.
Privacy	The Office of the Privacy Commissioner of Canada describes "privacy" as "... the right to control access to one's person and information about one's self. The right to privacy means that individuals get to decide what and how much information to give up, to whom it is given, and for what uses." The Treasury Board Secretariat's Directive on Privacy Practices (2013) defines privacy to be "the right of an individual to be left alone, to be free of unwarranted intrusions. It is also the right of an individual to retain control over his or her personal information and to know the uses, disclosures and whereabouts of that information."
Risk Scoring	The risk scoring involved an automated process for each passenger travelling to Canada. PAXIS contained four (4) risk templates which highlighted various information elements associated to a pattern. Values were assigned to specific information elements found within API PNR records. When PAXIS processed a traveller's API PNR record against the risk patterns, the values of matching elements found accumulated to a total score. If the total of the travellers score reached a pre-determined threshold limit under one or more of the

	four (4) established risk patterns, it was considered to be a high risk score. Those travellers were then provided to NRAC Targeting Officers for review.
Scenario	For each passenger travelling to Canada information is assessed against scenario criteria and elements to determine whether a traveller may be suspected of being high-risk and may require closer scrutiny. The criteria and elements are derived from analyzing enforcement information, tactical and operational enforcement information as well as intelligence information from law enforcement partners
Scenario Based Targeting (SBT)	Scenario based targeting is the application of a risk assessment methodology to identify high risk travellers whereby each scenario represents a specific combination of indicators of risk. Scenarios do not generate a cumulative score; rather, when a traveller's information matches all the criteria and elements of a scenario, they are considered to have potential risk which requires review by a targeting officer.
Target	The product of the targeting process that alerts appropriate CBSA personnel of an impending suspected risk to national security and/or public safety priorities.
Targeting	The process of identifying suspect high-risk people, goods and conveyances through a deductive reasoning process that utilizes intelligence products and technology to alert appropriate CBSA personnel of an impending suspected risk to ensure the interception of people, goods and conveyances that pose a risk to national security, including those related to public safety priorities.
Targeting Officer	A CBSA employee that identifies suspect high-risk people, goods and conveyances through the established targeting process and generates a target to alert appropriate CBSA personnel of an impending suspect risk to national security and/or public safety priorities.

SECTION 1 - OVERVIEW AND INITIATION

Report Objectives

This report is a Privacy Impact Assessment (PIA) for the SBT methodology within the risk assessment and targeting program of the CBSA. The objectives of this PIA are:

- to review the SBT business processes in order to identify the flow of personal information;
- to analyze the collection, use, disclosure and retention of SBT-related personal information;
- to determine if there are privacy risks associated with SBT methodology; and,
- to provide recommendations on the mitigation or elimination of any resulting risks.

The information presented in this report follows the Treasury Board of Canada Secretariat (TBS) *Directive on Privacy Impact Assessment (2010)*.

The purpose of a PIA process is to ensure that privacy is considered throughout the project development cycle. The results of a PIA are a documented guarantee that privacy issues have been identified and adequately addressed.

Government Institution: Canada Border Services Agency, Pre-Border Programs Branch

Government Official Responsible for the Privacy
 Impact Assessment

CBSA Vice President Programs Branch

Head of the government institution / Delegate for
 section 10 of the *Privacy Act*

CBSA ATI and Privacy Director

Approach to the Report

The approach to completing this PIA included a review of related documentation and meetings among CBSA officials. The advent of the use of SBT methodology was reviewed, summarized and analysed. Further enhancements to the SBT methodology may occur in the future pertaining to analytics and trend and pattern analysis.

Name of Program or Activity of the Government Institution:

Advance Passenger Information/Passenger Name Record (API/PNR) Program

Scenario-based targeting relies on the use of API/PNR information which is managed by the API/PNR Program and referenced within this PIA document. The API/PNR Program falls under "Risk Assessment" of the CBSA's 2011-2012 Program Activity Architecture of which "Targeting" is a sub activity.

Description of Program or Activity:

The Targeting Program identifies people that are bound for Canada that may pose a threat to the security and safety of Canada. The CBSA uses automated advance information sources from carriers to identify people who may pose a threat to Canada. Advance Passenger Information (API) provides the CBSA with electronic pre-arrival information on people that can be used to perform risk assessments in advance of their arrival in Canada. Known threats are identified when there is a match against an enforcement database entry. People identified as posing a threat to Canada are referred for verification and examination upon their arrival at a port of entry.

Description of the class of records associated with the program or activity:

Advance Passenger Information/Passenger Name Record (API/PNR) Program

Description: Describes records related to the API/PNR Program. May include records related to the establishment or use of electronic systems used to administer or manage the program including the Passenger Information System (PAXIS), the Integrated Customs Enforcement System (ICES) and Citizenship and Immigration Canada's Field Operations Support System (FOSS).

Document Types: Traveller's API/PNR Information Request Form, Memos, PAXIS system description and test packages, evaluation reports, passenger profile documentation, documentation from commercial carriers, compliance reviews and investigations and Memoranda of Understanding.

Class of Record Number: CBSA IST 001

- ☐ Proposal for a New Personal Information Bank
- ☒ Proposal to modify an existing Personal Information Bank - identify PIB registration number and current description:

•Advance Passenger Information / Passenger Name Record Program (API/PNR)

Description: This bank describes information about individuals seeking to enter Canada. Under Canadian law, all commercial carriers are required to provide Advance Passenger Information / Passenger Name Record (API/PNR) data relating to all individuals on board commercial conveyance bound for Canada. In the case of the Advance Passenger Information (API) personal information includes: name, date of birth, gender, citizenship or nationality and travel document information, reservation record locator number. With respect to the Passenger Name Record (PNR), personal information may include: name, traveller's reservation and travel itinerary, which could include point of origin and destination, dates and times of travel, address where the passenger will be residing while in Canada.

Class of Individuals: All individuals, including employees of the carrier, who are travelling on a commercial conveyance destined for Canada.

Purpose: The personal information is used to administer the Advance Passenger Information/Passenger Name Record program, which involves performing a risk assessment and assigning a risk-score to all individuals prior to their arrival in Canada. The authority to collect personal information is authorized by section 107.1 of the Customs Act, the Passenger Information (Customs) Regulations, paragraph 148(1)(d) of the Immigration and Refugee Protection Act, regulation 269 of the Immigration and Refugee Protection Regulations.

Consistent Uses: The information may be used for audit, evaluation, research, and / or statistical purposes. The information is routinely disclosed to RCMP and CSIS in accordance with 8(2)(e), when required. Passenger Information collected for Canada Border Services Agency's (CBSA) API/PNR program may be shared with U.S. Department of Homeland Security on a case-by-case basis pursuant to a memorandum of understanding.

Retention and Disposal Standards: Records will be retained for 3.5 years from date of travel and then the records are destroyed. Where the API and PNR information relates to a person who is the subject of an investigation in Canada the API/PNR information will be transferred to an enforcement database of the Canada Border Services Agency (CBSA) and be retained in that system for a period of no more than 6 years and destroyed after 6 years.

RDA Number: 90/002

Related Record Number: CBSA IST 001

TBS Registration: 005388

Bank Number: CBSA PPU 008

- ☐ Proposed new Standard Personal Information Bank
- ☐ Proposal to modify an existing Standard Personal Information Bank - identify Standard PIB number and current description:

Legal Authority for Program or Activity:

The authority to collect personal information is authorized by:

- section 107.1 of the *Customs Act*;
- the *Passenger Information (Customs) Regulations*;
- paragraph 148(1)(d) of the *Immigration and Refugee Protection Act*;
- regulation 269 of the *Immigration and Refugee Protection Regulations*, and
- *Protection of Passenger Information Regulations*.

Summary of the project, initiative, or change:

The SBT initiative is aligned with the CBSA's border vision and the Government of Canada's commitments under the *Beyond the Border Action Plan* to address threats earlier to enhance our security and accelerate the flow of legitimate goods and people.

This initiative is an important part of the Beyond the Border declaration, negotiated between Canada and the US. In 2011, as part of the *Beyond the Border Action Plan*, Canada committed to implementing a harmonized methodology for the screening of all air travellers. For CBSA, this involves the implementation of fully automated user managed scenario based rules.

The CCRA implemented the API/PNR program in October 2002 with the objective of mandating the collection of prescribed information from commercial air carriers for all air travellers for the purpose of risk assessing persons before they reach Canada's borders.

In 2003 and 2004, the CBSA established the High Risk Traveller Identification Initiative (HRTI) jointly with the US CBP to extend the API/PNR Program to identify high-risk air travellers. This protection was achieved through the pre-arrival risk assessment of traveller information within the risk scoring component of PAXIS.

Risk scoring was first implemented based on the above-noted joint agreement between Canada and the US. Both parties agreed to implement a risk scoring methodology within their automated passenger targeting systems to conduct risk assessment and targeting of unknown high-risk passengers flying into their respective countries.

Shortly after implementation, the US CBP changed their systems to implement a scenario based rules methodology. The US CBP encouraged and recommended that CBSA also change over to the scenario based rules approach.

After an extensive analysis of the effectiveness of the risk scoring methodology and the continued commitment to comply with agreements made with the US CBP, the CBSA undertook the replacement of risk scoring functionality with scenario-based rules functionality on a limited basis. Using API/PNR, historical enforcement trends and intelligence information, the scenarios will more effectively direct the focus on a smaller, more specific, segment of the travelling population who represent a potential high risk. SBT will also enable greater flexibility in scenario creation and maintenance that the risk scoring approach did not provide. It will be possible to create, modify or delete a scenario from PAXIS in near real time to support new, evolving or expired risk threats.

In January 2010, the Executive Policy Committee approved the implementation of a long term solution for SBT within PAXIS. PAXIS is a decision support tool that enables the CBSA to improve the use,

analysis, and dissemination of information to target, identify, and prevent those travellers linked to terrorism, terrorism-related crimes and other serious crimes that are transnational in nature from entering Canada.

SBT-related enhancements to PAXIS will increase the efficiency, effectiveness and accuracy of the Targeting Officer's otherwise manual and labour-intensive work, and thereby help facilitate the more efficient movement of legitimate people while safeguarding the border and the security of Canada. The enhancements also dramatically reduce scenario deployment times and costs enabling the CBSA to respond to imminent threats. Further, risk assessment will no longer be undertaken in two tiers (Regions and Headquarters), but will be consolidated into a single-tier model where the National Targeting Centre will undertake all targeting activities for all risks including SBT.

SBT methodology, once implemented, will include a flexible, user-managed risk tool that other CBSA traveller targeting initiatives can benefit from. This will be flexible enough to support expansion of targeting and risk assessment for other initiatives in the future, however, at this stage, such other initiatives are not yet identified and no decisions have been made that would result in the SBT tool being used by other CBSA initiatives.

The SBT methodology is scheduled to be implemented in three releases:

1. Release 1- 2014: Implementation of a user managed scenario application
2. Release 2- 2014: Changes to the PAXIS workflow and interface
3. Release 3- 2015: Enhanced and/or automated enforcement queries and any remaining requirements

This PIA assessed privacy concerns for functionality which was put forth for inclusion in the three releases but may need to be updated at a future date based on new or revised content to Release 3. The SBT initiative is subject to the *Customs Act, sections 7.1, and 107.1, the Immigration and Refugee Protection Act, paragraph 148(1)(d) and 149, the Immigration and Refugee Protection Regulations, Section 269, Passenger Information (Customs) Regulations, and the Protection of Passenger Information Regulations.*

The assessment of travellers for risk is not a new activity; this occurred with risk scoring. The use of SBT methodology is only a change in the process of assessing travellers for risk.

Program Activity and Organizational Operation

SBT relies, in part, on the use, access, retention and disclosure of API/PNR information which is managed by the API/PNR Program and described in this PIA for informational purposes. The API/PNR Program falls under "Risk Assessment" of the CBSA's 2011-2012 Program Activity Architecture of which "Targeting" is a sub activity.

Scope of this PIA

The Pre-Border Programs Division of the CBSA is undertaking the replacement of risk scoring functionality with scenario-based rules functionality using API/PNR that is processed and maintained in PAXIS.

The scope of this PIA is limited to assessing privacy risks associated with the deployment of the SBT methodology which will enable the CBSA to identify high-risk individuals and risk threats using intelligence-based recommendations and scenario-based risk rules.

This PIA is a sub-component of the API/PNR PIA and the HRTI PIA.

The API/PNR PIA focuses on information acquisition, retention and use while the HRTI PIA includes the previous risk scoring methodology and focuses on the disclosure of personal information to the US CBP. This SBT PIA focuses on the use of personal information.

The scope of this PIA is limited to the application of the SBT methodology only; most other aspects of personal information lifecycle management have been dealt with by the two other PIAs.

The personal information collected, managed, and disclosed by CBSA under the API/PNR Program is not part of the scope of this assessment, nor is information collected, managed, and disclosed to the US CBP. The scope of this PIA is limited to the assessment of risk to privacy using SBT to identify high-risk travellers within PAXIS.

The following table describes the scope of each PIA for clarity and to situate the SBT PIA in the overall privacy assessment context of API/PNR information.

PIA	Scope
Overarching Component: API / PNR PIA	Overarching PIA, that includes both the HRTI as well as the SBT PIA's. The scope of this PIA covers the collection, use, disclosure, retention and disposal of personal information collected for the API/PNR Program for air mode and retained in PAXIS. The scope of the API/PNR PIA report does not include the operation of ICES or FOSS, although personal information from these systems may be used for purposes of the API/PNR Program.
Sub Component: HRTI PIA	The scope of this PIA is limited to the CBSA responsibilities associated with the HRTI initiative and includes the previous risk scoring methodology and the sharing of API/PNR information with the US CBP.
Sub Components: SBT PIA	The scope of this PIA is limited to the replacement of risk scoring functionality with scenario-based rules functionality using API/PNR information.

SECTION 2 - RISK AREA IDENTIFICATION AND CATEGORIZATION

Type of Program or Activity	Level of Risk
Program or activity that does NOT involve a decision about an identifiable individual Personal information is used strictly for statistical / research or evaluations including mailing list where no decisions are made that directly have an impact on an identifiable individual. The Directive on PIA applies to administrative use of personal information. The Policy on Privacy Protection requires that government institutions establish an institutional Privacy Protocol for addressing non-administrative uses of personal information.	<input type="checkbox"/> 1
Administration of Programs / Activity and Services Personal information is used to make decisions that directly affect the individual (i.e. determining eligibility for programs including authentication for accessing programs/services, administering program payments, overpayments, or support to clients, issuing or denial of permits/licenses, processing appeals, etc...).	<input type="checkbox"/> 2

Compliance / Regulatory investigations and enforcement

☐ 3

Personal information is used for purposes of detecting fraud or investigating possible abuses within programs where the consequences are administrative in nature (i.e. a fine, discontinuation of benefits, audit of personal income tax file or deportation in cases where national security and/or criminal enforcement is not an issue).

Criminal investigation and enforcement / National Security

☒ 4

Personal information is used for investigations and enforcement in a criminal context (i.e. decisions may lead to criminal charges/sanctions or deportation for reasons of national security or criminal enforcement).

Details: In all cases, API/ PNR information collected by the CBSA will be used by authorities for purposes supporting the CBSA mandate that includes both the referral of high risk individuals for secondary processing at a port of entry in Canada and the trend analysis for the development of scenarios. The activity provides authorized CBSA personnel access to information to perform risk assessment functions for targeting and intelligence purposes. The deployment of the SBT methodology replaces the risk scoring methodology previously applied. With either the risk scoring approach or the SBT approach, the same personal information is involved. With SBT, it is an automated process based on pre-determined scenarios as opposed to an automated process based on risk score thresholds that assists the Targeting Officer to make a determination regarding the issuance of a target.

Type of Personal Information Involved and Context

Level of Risk

- Only personal information, with no contextual sensitivities, collected directly from the individual or provided with the consent of the individual for disclosure under an authorized program. ☐ 1
- Personal information, with no contextual sensitivities after the time of collection, provided by the individual with consent to also use personal information held by another source. ☐ 2
- Social Insurance Number, medical, financial or other sensitive personal information and/or the context surrounding the personal information is sensitive. Personal information of minors or incompetent individuals or involving a representative acting on behalf of the individual. ☐ 3
- Sensitive personal information, including detailed profiles, allegations or suspicions, bodily samples and/or the context surrounding the personal information is particularly sensitive. ☒ 4

Details: API information is basic information collected by commercial air carriers when a passenger checks in for departure to Canada. PNR information is information about a traveller's flight itinerary and flight information (e.g., method of payment, travel agent) that resides in an airline's reservation system.

The personal information involved in SBT is not collected directly from the individual by CBSA. It is collected by CBSA from the air carrier as API/PNR personal information as prescribed under the API/PNR Program and is subsequently applied to the scenario based risk rules to identify persons who are or who may be involved with or connected to terrorism or terrorism-related crimes or other serious crimes, including organized crime, that are transnational in nature. Personal information from external sources such as the RCMP's CPIC and Interpol is also collected by CBSA for the risk assessment.

The approach taken by CBSA is to only retain summary information from enforcement queries but enable access to more detailed information, as required, for the Targeting Officer to make a determination whether to issue a target. Depending on the information and the source, a key (record identifier), unique number and/or summary of the information is retained in PAXIS. If a key is used, the information itself is not retained in PAXIS but can be re-accessed. This is, in part, to ensure that the CBSA is accessing current and accurate information about the traveller from those other sources. While most of the personal information used for SBT is considered to be of a low sensitivity, information about a traveller's outstanding warrants or other information such as criminal records, obtained from CPIC or Interpol may be considered sensitive. If the Targeting Officer decides to issue a Target, new personal information about the individual is created that reflects the risk assessment of the individual. This is not a new outcome for the targeting process and occurred with risk scoring methodology as well. The target will allow the BSO at POE to take action to confirm or negate any further risk.

Program or Activity Partners and Private Sector Involvement

Level of Risk

- Within the CBSA (amongst one or more programs within the CBSA) ☒ 1
- With other federal institutions ☒ 2
- With other or a combination of federal/ provincial and/or municipal government(s) ☐ 3

Private sector organizations or international organizations or foreign governments

☒ 4

Details: The SBT involves using personal information from other components obtained from CBSA, federal partners (RCMP, CSIS, CIC) and the private sector (airlines). It also involves obtaining, using and disclosing personal information from, and disclosing personal information to, the US CBP. The disclosure of information to the US CBP was previously assessed in the HRTI PIA.

Duration of the Program or Activity

Level of risk

One time program or activity

☐ 1

Typically involves offering a one-time support measure in the form of a grant payment as a social support mechanism.

Short-term program

☐ 2

A program or activity that supports a short-term goal with an established "sunset" date.

Long-term program

☒ 3

Existing program that has been modified or is established with no clear "sunset".

Details: Launched in 2002, the API/PNR program was originally developed as a joint initiative between CIC and the Canada Customs and Revenue Agency (CCRA) to improve risk management procedures. The responsibility for the program shifted, however, when the CBSA was created on December 12, 2003. The program is currently operational and will continue into the foreseeable future. The High Risk Traveller Initiative from 2003 will continue with SBT functionality.

Program Population

Level of Risk

The program affects certain employees for internal administrative purposes.

☐ 1

The program affects all employees for internal administrative purposes.

☐ 2

The program affects certain individuals for external administrative purposes.

☒ 3

The program affects all individuals for external administrative purposes.

☐ 4

Details: Under Canadian law, all commercial carriers are required to provide the CBSA with API/PNR information relating to all persons travelling to Canada by air. Airlines collect API information when passengers and crew check in; PNR information is received from airline flight reservation and departure control systems.

Technology and Privacy

6.1 Does the new or modified program or activity involve the implementation of a new electronic system, software or application program including collaborative software (or groupware) that is implemented to support the program or activity in terms of the creation, collection or handling of personal information?

☒ YES
☐ NO

6.2 Does the new or modified program or activity require any modifications to IT legacy systems and / or services?

☒ YES
☐ NO

6.3 Does the new or modified program or activity involve the implementation of one or more of the following technologies:

6.3.1 Enhanced identification methods:

This includes biometric technology (i.e. facial recognition, gait analysis, iris scan, fingerprint analysis, voice print, radio frequency identification (RFID), etc...) as well as easy pass technology, new identification cards including magnetic stripe cards, "smart cards" (i.e. identification cards that are embedded with either an antenna or a contact pad that is connected to a microprocessor and a memory chip or only a memory chip with non-programmable logic).

☐ YES
☒ NO

Details:

6.3.2 Use of Surveillance:

This includes surveillance technologies such as audio/video recording devices, thermal imaging, recognition devices, RFID, surreptitious surveillance / interception, computer aided monitoring including audit trails, satellite surveillance etc.

☐ YES
☒ NO

Details:

6.3.3 Use of automated personal information analysis, personal information matching and knowledge discovery techniques:

For the purposes of the Directive on PIA, CBSA is to identify those activities that involve the use of automated technology to analyze, create, compare, cull, identify or extract personal information elements. Such activities would include personal information matching, record linkage, personal information mining, personal information comparison, knowledge discovery, information filtering or analysis. Such activities involve some form of artificial intelligence and/or machine learning to uncover knowledge (intelligence), trends/patterns or to predict behaviour.

☒ YES
☐ NO

Details: SBT is not an automated personal information analysis. The scenario based risk rules are not using an analytical methodology but rather a comparison methodology in that passenger information is matched against the scenario criteria and the various elements of the criteria and a match either exists or does not.

Data matching is also involved when scenarios are simulated in a non-production environment. The outcome from the simulation though does not contain personal information only aggregate results and is intended to assess the potential impact on border and targeting operations that would result from the introduction of new or modified targeting scenarios.

Personal Information Transmission

Level of Risk

The personal information is used within a closed system.

☐ 1

No connections to Internet, Intranet or any other system. Circulation of hardcopy documents is controlled.

The personal information is used in system that has connections to at least one other system.

☒ 2

The personal information is transferred to a portable device or is printed.

☒ 3

USB key, CD-Rom, laptop computer, any transfer of the personal information to a different medium.

The personal information is transmitted using wireless technologies.

☐ 4

Details: Personal information may be transmitted through secure connections when CPIC and Interpol queries provide results. There are also network connections within CBSA between PAXIS, FOSS and ICES. Personal information can be printed from PAXIS but no personal information is transferred to portable devices. Any personal information that is printed is subject to CBSA information management policies including:

- *Administrative Guidelines for the Provision to Others, Allowing Access to Others and Use of Advance Passenger Information (API) and Passenger Name Record (PNR) Data*
<http://www.cbsa-asfc.gc.ca/publications/dm-md/d1/d1-16-3-eng.pdf>
- *Canadian Police Information Centre (CPIC) Policy*
http://www.cpic-cipc.ca/pdfs/cpicpolicy_e.pdf
- *CBSA Code of Conduct*
http://atlas/hrb-dgrh/pol/sr-rt/code/cc_eng.asp
- *CBSA Security Policies, Chapter 6*
http://atlas/cb-dgc/pol/cm-mc/sv-vs/index_eng.asp
- *A Guide to the Transmission, Storage and Destruction of Protected and Classified Information*
http://atlas/cb-dgc/sec/pcinfo_e.asp
- *International arrangements to share API/PNR data*
http://www.cbsa.gc.ca/security-securite/api_ipv-eng.html
- *Policy Guidelines on the Disclosure of Customs Information: Section 107 of the Customs Act*
<http://www.cbsa-asfc.gc.ca/publications/pub/bsf5150-eng.html>

Risk Impact to the CBSA

Level of Risk

Managerial harm.

☒ 1

Processes must be reviewed, tools must be changed, change in provider / partner.

Organizational harm.

☒ 2

Changes to the organizational structure, changes to the organizations decision-making structure, changes to the distribution of responsibilities and accountabilities, changes to the program activity architecture, departure of employees, reallocation of HR resources.

Financial harm.

☒ 3

Lawsuit, additional moneys required reallocation of financial resources.

Reputation harm, embarrassment, loss of credibility.

☒ 4

Decreased confidence by the public, elected officials under the spotlight, institution strategic outcome compromised, government priority compromised, impact on the Government of Canada Outcome areas.

Details: The risks to the CBSA resulting from a breach or misuse of personal information encompass the possibilities described above.

Risk Impact to the Individual or Employee	Level of Risk
Inconvenience.	<input checked="" type="checkbox"/> 1
Reputation harm, embarrassment.	<input checked="" type="checkbox"/> 2
Financial harm.	<input checked="" type="checkbox"/> 3
Physical harm.	<input type="checkbox"/> 4
Details: No new risks to individuals are caused by the deployment of the SBT.	

A) Beyond the Border Privacy Principles

Risk to privacy

Purpose: Have the purposes for which personal information is collected and disclosed been identified and documented?

☒ YES
☐ NO

The practices associated with the collection of personal information are not changing as a result of the deployment of SBT and are not directly related to this PIA. However, PIB CBSA PPU 008 explains the purposes of the collection of API/PNR and Target-related personal information which is used in the SBT process. In addition, the purposes of the collection, use and disclosure are outlined in the API/PNR PIA, the High-Risk Traveller Identification Initiative PIA and this PIA (Executive Summary, Overview and Initiation and Summary of the Project, Initiative or Change). However, the current API/PNR PIB does not fully reflect all of the legal authorities.

Relevant and Necessary/Proportionate: Is the personal information collected: necessary, proportionate and related to an operating program or activity?

☒ YES
☐ NO

The personal information that is collected is necessary for the targeting process and is related to the API/PNR Program and HRTI. The CBSA has authority to collect and use all elements of personal information in its targeting processes as outlined in *Privacy Act* Principle 2: Collection of Personal Information of the API/PNR Project PIA and in Section 5 – privacy compliance analysis and SECTION 4 - FLOW OF PERSONAL INFORMATION of this PIA Report.

Integrity and Data Quality: Are all steps taken to ensure continuing accuracy and completeness of personal information, including any caveats or conditions attached to such information?

☒ YES
☐ NO

The issuance of queries to additional enforcement databases is in itself a process of determining the accuracy and completeness of personal information and while this practice was undertaken with the risk scoring approach, it is now automatically undertaken with the SBT methodology. Further details regarding the accuracy of the SBT-related personal information can be found at item 8.1.

Non-Discrimination: Is the Canadian *Privacy Act* and the Statement of Privacy Principles applied to all individuals on an equal basis without unlawful discrimination?

☒ YES
☐ NO

SBT methodology is automatically applied to all travellers onboard international flights bound for Canada without discrimination.

Information Security: Have security procedures for the collection, transmission, storage and disposal of personal information, and access to it, been documented?

☒ YES
☐ NO

An IT Security Risk Mitigation Analysis was conducted in 2013. It was focused on Scenario Based Targeting for High Risk Travellers – Transition Architecture R1 & R2. Further safeguards-related information can be found at 13. Safeguards - Threat and Risk Assessment and at SECTION 2 - RISK AREA IDENTIFICATION AND CATEGORIZATION.

Accountability:

☒ YES
☐ NO

1. Has the accountability of the program custodian for personal information been documented?

Although the Pre-Border Program Directorate, the functional program authority for SBT, has policy oversight for personal information related to SBT, the CBSA's Access to Information Coordinator has full authority delegated by the head of the institution for the administration of the *Privacy Act*. In June, 2012, the CBSA implemented the role of a Chief Privacy Officer. A director general, the Chief Privacy Officer's mission is to support the CBSA's vision for fostering and maintaining a strong Agency-wide privacy governance structure

which takes into account the privacy rights of individuals, the obligations of the *Privacy Act* and related policies, and the Agency's need to collect, retain, use, disclose and dispose of personal information. Privacy is a shared responsibility. In order to bring executive-level focus to privacy risks, the Chief Privacy Officer chairs and is supported by a CBSA privacy oversight committee of key executives drawn from across the organization. In these ways, the CBSA ensures accountability for the personal information it collects, uses, discloses and retains.

2. Are there oversight and review mechanisms implemented or available to ensure accountability?

☒ YES
☐ NO

In addition to the Chief Privacy Officer role noted above, the Privacy Commissioner of Canada has a mandate to conduct compliance reviews of the privacy practices of government institutions as the practices relate to the collection, retention, accuracy, use, disclosure and disposal of personal information by government institutions subject to the Act. The Commissioner has the powers of an ombudsman and can make recommendations with respect to any matter which has been investigated or reviewed. In addition, the Commissioner can report on institutional activities in annual or special reports to Parliament.

Effective Oversight:

1. Has the custody and control of personal information been determined and documented?

☒ YES
☐ NO

Please refer to SECTION 5 - PRIVACY COMPLIANCE ANALYSIS for details on the custody and control of SBT-related personal information.

2. Does the Agency have clear authority to collect, retain, use, and disclose such personal information?

☒ YES
☐ NO

Refer to CBSA PPU 008 for details on the authority to collect, use, retain and disclose the personal information. Refer also to item 1 at SECTION 5 - PRIVACY COMPLIANCE ANALYSIS for further details.

Individual Access and Rectification: Are there documented procedures developed or planned for how to initiate privacy requests or requests for the correction of personal information?

☒ YES
☐ NO

CBSA follows routine procedures for responding to privacy requests or requests for correction of personal information and publishes information for the public at http://www.cbsa-asfc.gc.ca/security-securite/api_ipv_note-eng.html regarding how travellers can seek access to the API/PNR personal information. When a query result provides information that is displayed, PAXIS retains a key, unique number and/or a summary of the information but not the full detailed information itself. When a SBT query to another database results in the viewing of personal information, by the Targeting Officer, but not the retention of that information, it raises a question as to how the individual concerned would ever access his or her SBT-related personal information. In such an extremely unlikely situation, CBSA authorities could recreate the previously displayed information in response to a request filed by an individual under s.s 12 (1) of the *Privacy Act* for his or her personal information. In every case, the personal information would be evaluated through existing routine processes and could be withheld from disclosure under various exemption provisions contained in the same Act due to its confidential nature.

CBSA targeting officials are not in a position to make changes to any of the personal information used in the process of determining to issue a target because the information is sourced from systems managed by other components of the CBSA or by external parties. A request for correction for personal information residing in any of the systems that feed the SBT could be made to the owners of those systems and routine procedures would follow.

Transparency and Notice:

Should notice need to be limited for national security or law enforcement reasons, such as the protection of an

☒ YES
☐ NO

ongoing investigation or the protection of victims or witnesses, the limitation on notice should be consistent with all applicable laws of Parliament.

1. Is there a privacy notice at the collection stage that identifies the specific purposes for the collection, the authority for doing so and the individual serving as official contact?

Airline carriers are required to become certified by CBSA with respect to the API/PNR process and are required to provide traveller's with access to a privacy notice statement. In addition, CBSA publishes an API/PNR privacy notice at http://www.cbsa-asfc.gc.ca/security-securite/api_ipv-eng.html.

2. If personal information is not disclosed with the consent of the individual, has the specific authority for disclosure been identified?

☒ YES
☐ NO

Refer to item 1 at SECTION 5 - PRIVACY COMPLIANCE ANALYSIS for details related to the CBSA's specific legal authorities for the collection, use and disclosure of SBT-related personal information.

Redress: Are the complaint procedures for the proposed program or service consistent with legislated requirements?

☒ YES
☐ NO

Subsection 29(1) of the *Privacy Act* describes how the OPC receives and investigates complaints from individuals in respect to their personal information held by a government institution. CBSA responded to 54 such privacy complaints during 2011-2012 and has implemented new electronic processes and tools for responding to privacy complaints.

Restrictions on Onward Transfers to Third Countries:

Where personal information is provided, in accordance with relevant domestic law, by a competent authority of the United States or Canada (the originating country) to a competent authority of the other nation (the receiving country), the competent authority of the receiving country is to authorize or carry out an onward transfer of this information to a third country only if consistent with the domestic law of the receiving country, and in accordance with existing applicable international agreements and arrangements.

In the absence of such international agreements and arrangements, the receiving country may transfer the personal information to a third country when consistent with the domestic law of the receiving country, in which case the originating country is to be notified:

- o prior to the transfer; or
- o as soon as reasonably possible after the transfer in the case of exigent circumstances.

1. Has the information been collected from a government authority in United States?

As indicated At SECTION 5 - PRIVACY COMPLIANCE ANALYSIS, SECTION 4 - FLOW OF PERSONAL INFORMATION and SECTION 3 - ANALYSIS OF PERSONAL INFORMATION ELEMENTS, the SBT process relies, in part, on personal information collected from the USCBP when a traveller's API/PNR information matches a scenario.

2. Will the information be transferred to a third country?

☒ YES
☐ NO
☐ YES
☒ NO
☒ YES
☐ NO

Retention:

1. Is the personal information scheduled for retention and disposition?

Personal Information Bank CBSA PPU 008 outlines the retention and disposition practices.

2. Is personal information disclosed for secondary use, not supported by legislative authority?

☐ YES
☒ NO

SECTION 3 - ANALYSIS OF PERSONAL INFORMATION ELEMENTS

Personal Information Elements and Sub-elements

API Cluster

Category Of Personal Information	Personal Information Element	Personal Information Sub-Element	Format	Purpose / Necessity of Element
<i>Name</i>	Name	The passenger's surname, first name, middle name and initial or initials, if any	Electronic	Necessary to help establish identities of passengers and crew coming to Canada.
<i>Date of Birth</i>	Date of birth	The passenger's date of birth	Electronic	Necessary to help establish identities of passengers and crew coming to Canada.
<i>Gender</i>	Gender	The passenger's gender	Electronic	Necessary to help establish identities of passengers and crew coming to Canada.
<i>Citizenship or Nationality</i>	Citizenship or nationality	The passenger's citizenship or nationality, or failing either of these, the country that issued travel documents to the passenger for the flight	Electronic	Necessary to help establish identities of passengers and crew coming to Canada.
<i>Travel Document</i>	Type of travel document that identifies them, the name of the country in which the travel document was issued and the number on the travel document		Electronic	Necessary to help establish identities of passengers and crew coming to Canada.
<i>E-Ticket Information</i>	Reservation record locator number (if any)		Electronic	Necessary to help establish identities of passengers and crew coming to Canada.
<i>Crew detailed information</i>	Crew member status (in the case of a person in charge of the commercial conveyance)	Indicates traveller's status as a crew member	Electronic	Necessary to help establish identities of passengers and crew coming to Canada.

Scenario Based Targeting for High Risk Travellers

PIA v14
 Protected B

Category Of Personal Information	Personal Information Element	Personal Information Sub-Element	Format	Purpose / Necessity of Element
	or any other crew member without a reservation record locator number)			

PNR Cluster

Category Of Personal Information	Personal Information Element	Personal Information Sub-Element	Format	Purpose / Necessity of Element
Name	Name	The passenger's surname, first name, middle name and initial or initials, if any	Electronic	Necessary to help assess potential risk posed by a passenger.
	API information		Electronic	Necessary to help assess potential risk posed by a passenger.
E-Ticket Information	PNR record locator code	The PNR number As available in the traveller's Passenger Name Record in the carrier's airline reservation system ¹	Electronic	Necessary to help assess potential risk posed by a passenger.
E-Ticket Information	Date of intended travel	The travel date for the flight	Electronic	Necessary to help assess potential risk posed by a passenger.
E-Ticket Information	Date of reservation	The date on which the PNR was created	Electronic	Necessary to help assess potential risk posed by a passenger.
E-Ticket Information	Date of ticket issuance	The date on which the passenger's ticket for the flight was issued	Electronic	Necessary to help assess potential risk posed by a passenger.
E-Ticket Information	Travel agencies	If applicable, the names of the travel agency that made the travel arrangements	Electronic	Necessary to help assess potential risk posed by a passenger.

¹ Not all carriers have all PNR elements available and are only mandated to provide what they retain in their reservation systems.

Scenario Based Targeting for High Risk Travellers

PIA v14
 Protected B

Category Of Personal Information	Personal Information Element	Personal Information Sub-Element	Format	Purpose / Necessity of Element
E-Ticket Information	Travel agent	If applicable, the name of the travel agent that made the travel arrangements	Electronic	Necessary to help assess potential risk posed by a passenger.
E-Ticket Information	Contact telephone information	The phone numbers of the passenger and, if applicable, the phone number of the travel agency that made the travel arrangements	Electronic	Necessary to help assess potential risk posed by a passenger.
E-Ticket Information	Billing address	The address of the passenger and, if applicable, of the travel agency that made the travel arrangements	Electronic	Necessary to help assess potential risk posed by a passenger.
E-Ticket Information	All forms of payment information	The manner in which the ticket was paid for	Electronic	Necessary to help assess potential risk posed by a passenger.
E-Ticket Information	Frequent Flyer Information (limited to miles flown and address(es))		Electronic	Necessary to help assess potential risk posed by a passenger.
E-Ticket Information	Ticketing Field Information	The date, if any, by which the ticket for the flight had to be paid for to avoid cancellation of the reservation, or the date, if any, on which the request for a reservation was queued from the transportation company to the ticketing office	Electronic	Necessary to help assess potential risk posed by a passenger.
E-Ticket Information	Ticket number	The number assigned to the passenger's ticket for the flight	Electronic	Necessary to help assess potential risk posed by a passenger.
E-Ticket Information	Split/divided PNR		Electronic	Necessary to help assess potential risk posed by a passenger.
E-Ticket Information	Go show information (ticket purchase without a reservation)	If applicable, a notation that the passenger arrived at the departure gate with a ticket but without a reservation for the flight	Electronic	Necessary to help assess potential risk posed by a passenger.
E-Ticket Information	No show history		Electronic	Necessary to help assess potential risk posed by a passenger.

Scenario Based Targeting for High Risk Travellers

PIA v14
 Protected B

Category Of Personal Information	Personal Information Element	Personal Information Sub-Element	Format	Purpose / Necessity of Element
<i>E-Ticket Information</i>	All travel Itinerary Information	The itinerary cities, being all points where the passenger will embark or disembark, car rental segments, and hotel segments.	Electronic	Necessary to help assess potential risk posed by a passenger.
<i>E-Ticket Information</i>	Standby Information		Electronic	Necessary to help assess potential risk posed by a passenger.
<i>E-Ticket Information</i>	Other names on PNR		Electronic	Necessary to help assess potential risk posed by a passenger.
<i>E-Ticket Information</i>	Order of check in		Electronic	Necessary to help assess potential risk posed by a passenger.
<i>E-Ticket Information</i>	Bag tag numbers	The baggage tag number associated with the passenger's checked baggage.	Electronic	Necessary to help assess potential risk posed by a passenger.
<i>E-Ticket Information</i>	Seat information	Any stated seat request in respect of the flight	Electronic	Necessary to help assess potential risk posed by a passenger.
<i>E-Ticket Information</i>	Seat number	Any seat assignment on the flight that was selected for the passenger prior to departure	Electronic	Necessary to help assess potential risk posed by a passenger.
<i>E-Ticket Information</i>	One way tickets	If applicable, a notation that the passenger's ticket for the flight is a one-way ticket	Electronic	Necessary to help assess potential risk posed by a passenger.

Other Databases

The scope of the SBT PIA assessment does not include the operation of FOSS, CPIC, ICES, Interpol, or ICS, although personal information from these systems may be used for purposes of SBT. It must be noted that the results of queries made to all systems are rendered and presented to system users in a seamless and integrated fashion; however, the detailed results of the queries are not stored within PAXIS. A key, unique number and/or summary, indicating that a hit resulted from any one of the queries, is recorded in PAXIS. It is important to note that the queries to the other databases are a current practice, currently accessed manually by a Targeting Officer, as part of the targeting process. The SBT initiative includes enhancements to simply automate the queries.

Database Queried by PAXIS	Database Operator	Description of PAXIS Query Process
Field Operation Support System (FOSS)	CBSA / CIC	An electronic query from PAXIS to FOSS is made to determine if an individual has an immigration related activity record in FOSS. If results are returned, a summary of the information is retained in PAXIS. The targeting officer may view limited details of the individual's FOSS record. This is a use of previously collected or compiled personal information.
Canadian Police Information Centre (CPIC)	RCMP	An electronic query from PAXIS to CPIC is made to determine if an individual has tactical and or operational law enforcement information in CPIC. This may include but not be limited to warrants, criminal records, court proceedings, etc. If a result is returned, an indicator of that result is placed in PAXIS. The targeting officer may view the CPIC record. This is a process that is currently applied manually in the CPIC Web application, and is not changing as result of the SBT initiative, except to be automated for efficiencies.
Integrated Custom Enforcement System (ICES)	CBSA	An electronic query from PAXIS to ICES is made to determine if an individual has an enforcement record in ICES. If results are returned, an indicator of a result is placed in PAXIS and the targeting officer may view a synopsis of the individual's enforcement records deemed to be a match or a close match. This represents a use of previously collected personal information that is not changing as a result of SBT. This occurred with risk scoring too.
Integrated Custom System (ICS) Global Enrollment Component		An electronic query from PAXIS to Global Enrollment Component (GEC) is made to determine if a traveller is an active member of a trusted traveller program; CANPASS Air or NEXUS

Scenario Based Targeting for High Risk Travellers

PIA v14
 Protected B

Interpol	RCMP	An electronic query from PAXIS to CPIC will result in responses indicating Interpol criminality and warrants. A positive result will provide an ID number which users will be required to manually query to retrieve details.
Integrated Custom System (ICS) Passage History	CBSA	An electronic query from PAXIS to ICS Passage History is made to determine if an individual has any previous passage crossings and secondary referrals.
Intelligence Management System (IMS)	CBSA	An electronic query from PAXIS to IMS is made to determine if an individual is identified as being part of a project or case within the intelligence stream. If a result is returned, an indicator is placed in PAXIS. The Targeting Officer can view detailed results.
Automated Targeting System (ATS)	US CBP	API/PNR information is shared with this organization pursuant to the Memorandum of Understanding for the Automated Exchange of Lookouts and the Exchange of Advance Passenger Information (API) MOU that has been in place since 2005 for the exchange of high-risk traveler information.

4.3 Internal Use and Disclosure

Internal Use	
Program	Personal information bank
National Targeting Centre (NTC)	CBSA PPU 008 (API/PNR)

4.4 External Use and Disclosure

External Use	
RCMP, CSIS	The information is disclosed to RCMP and CSIS in accordance with 8(2)(e), when required and as defined in Section 9 of the PPIR. This process is not a new process caused by the application of SBT. This existed with risk scoring.
Non-federal institutions and private sector	
US CBP	API and PNR information on individual travellers matching predetermined scenarios is shared between CBSA and US CBP to facilitate more detailed examination of high-risk individuals arriving by air in Canada or the US. This process is not a new process caused by the application of SBT. This existed with risk scoring.

4.5 Retention / Storage

Retention & Storage	
CBSA	Records will be retained for 3.5 years by the CBSA from date of travel and then the records are destroyed. Where the API and PNR information relates to a person who is the subject of an investigation in Canada API and PNR information may be transferred to an enforcement database of the CBSA (including target information) and be retained in that system for a period of no more than 6 years and destroyed after 6 years.
Non-federal institutions and private sector	
US CBP	NA

4.6 Other Possible Considerations

Federal government Institution responsible for program or activity:		
Identify Groups or Areas / or Divisions	Where appropriate - positions who have access or use the personal information	Geographical Location

Pre-Border Programs Directorate Traveller Targeting and Advance Information Programs Division	Program Advisor/Officer Program Manager Scenario Administrator	Ottawa
National Border Operations Centre / National Targeting Centre	Targeting Officer Intelligence Officer Supervisor See also designated users in CBSA D-Memorandum-1-16-3	Ottawa
Business Systems Support Directorate/ Business Systems Support Enforcement Division	Technical Support	Ottawa
Information Science and Technology Branch/ Solutions Directorate/ Enforcement Systems	Developer/Systems Analyst	Ottawa
Other federal government Institution responsible for program or activity:		
N/A		
Non Federal Institution or Private Sector:		
N/A		

SECTION 5 - PRIVACY COMPLIANCE ANALYSIS

1. Legal Authority For Collection Of Personal Information

Has a legal authority been identified for the collection of personal information for this program or activity?

Statutory reference: Section 4 of Privacy Act (Section 4 has been interpreted to mean that a legal authority must be established for a collection of personal information, but section 4 does not provide legal authority for such a collection).

Policy reference: Section 6.2.6 of Directive on Privacy Practices

Yes

- 1.1 ☒ Specify the legal authority and briefly explain its connection to the program or activity or how it permits the collection of the personal information:

The legal authority to collect the API-PNR information is supported by the API-PNR Program and mandated through the Customs Act and the supporting regulations. The collection of pre-arrival traveller information allows for the CBSA to risk assess travellers earlier in the continuum to ensure appropriate measures can be taken to negate risk. SBT provides an updated risk assessment methodology to better identify potential high risk travellers, as well, aligns the CBSA risk methodology with the US CBP per the commitment made under the Border Action Plan. (Beyond the Border Sub-Initiative 11(b))

Section 7.1 of the Customs Act:

Obligation to provide accurate information

7.1 Any information provided to an officer in the administration or enforcement of this Act, the Customs Tariff or the Special Import Measures Act or under any other Act of Parliament that prohibits, controls or regulates the importation or exportation of goods, shall be true, accurate and complete.

Section 107.1 Customs Act

Passenger information

107.1 (1) The Minister may, under prescribed circumstances and conditions, require any prescribed person or prescribed class of persons to provide, or to provide access to, within the prescribed time and in the prescribed manner, prescribed information about any person on board a conveyance.

The *Customs Act* can be reviewed at <http://laws.justice.gc.ca/en/c-52.6/45587.html>

Paragraph 148(1)(d) of the Immigration and Refugee Protection Act

Obligations of operators of vehicles and facilities

148 (1) A person who owns or operates a vehicle or a transportation facility, and an agent for such a person, must, in accordance with the regulations,

(d) provide prescribed information, including documentation and reports;

The *Immigration and Refugee Protection Act* can be viewed at <http://laws-lois.justice.gc.ca/eng/acts/I-2.5/FullText.html#h-77>

Section 269 of the Immigration and Refugee Protection Regulations

Advance passenger information

269. (1) On the request of an officer, a commercial transporter must provide on departure of their commercial vehicle from the last point of embarkation before arriving in Canada the following information in writing on each person carried:

- (a) their surname, first name and initial or initials of any middle names;
- (b) their date of birth;
- (c) the country that issued them a passport or travel document or, if they do not have a passport or travel document, their citizenship or nationality;
- (d) their gender;
- (e) their passport number or, if they do not have a passport, the number on the travel document that identifies them; and
- (f) their reservation record locator or file number.

The *Immigration and Refugee Protection Regulations* can be viewed at <http://laws-lois.justice.gc.ca/eng/regulations/SOR-2002-227/FullText.html#h-121>

Sections of the Protection of Passenger Information Regulations

- Sub-paragraph 5(1)(a)(ii) for the purposes of conducting trend analysis or developing future risk indicators in relation to the purpose referred to in section 3;
- Sub-paragraph 7(2)(b) access to the PNR information in respect of that person, other than their

name, may be provided to an authorized CBSA official for the purposes of conducting trend analysis or developing future risk indicators in relation to the purpose referred to in section 3;

- Sub-paragraph sec7(4)(a) access to the data elements contained in the PNR information that could serve to identify the person to whom the information relates may be provided to an intelligence official for the purpose referred to in section 3 if such access is approved by the President of the Agency;
- Sub-paragraph sec 7(4)(b) access to the PNR information, other than the data elements referred to in paragraph (a), may be provided to an authorized CBSA official for the purposes of conducting trend analysis or developing future risk indicators in relation to the purpose referred to in section 3, and
- Sub-paragraph sec 3: API information and PNR information may be retained by the Agency for the purpose of identifying persons who are or may be involved with or connected to terrorism or terrorism-related crimes or other serious crimes, including organized crime, that are transnational in nature.

Disclosure to Canadian Government Departments

Section 9. API information and PNR information retained by the Agency in the PAXIS system may be disclosed by the Agency to any Canadian government department for the purposes of the Act if

- (a) an official of the Agency has determined that the information
 - (i) relates to terrorism or crimes referred to in section 3, or
 - (ii) relates to an objective set out in section 3 of the Act and is required
 - (A) in order to comply with a subpoena or warrant issued by, or an order made by, a court, person or body with jurisdiction in Canada to compel the production of the information, or
 - (B) for the purposes of any judicial proceedings in Canada;
- (b) that department has undertaken to provide the information with the same type of protection as that provided by the Agency and not to further disclose the information without the permission of the Agency, unless required by law to do so; and
- (c) only the data elements contained in the information that are necessary for the purpose for which it is being disclosed are provided.

The Protection of Passenger Information Regulations can be viewed at <http://laws-lois.justice.gc.ca/eng/regulations/SOR-2005-346/FullText.html>

Sections of the Passenger Information (Customs) Regulations

- Section 2 describes what is a prescribed class of persons (e.g., commercial carriers, travel agents, owners and operators of reservation systems)
- Section 3 prescribes the information in respect of a person on board a commercial conveyance as defined in the regulation
- Sub-section 4 (1) requires the provision of the prescribed information to the CBSA (Minister's representative)

The Passenger Information (Customs) Regulations can be viewed at <http://laws-lois.justice.gc.ca/eng/regulations/SOR-2003-219/page-1.html#docCont>

- 1.2 ☒ Is the personal information collected directly related to an operating program or activity?

Details:

The SBT initiative is aligned with the CBSA's border vision and the Government of Canada's commitments under the *Beyond the Border Action Plan* to address threats earlier to enhance our security and accelerate the flow of legitimate goods and people.

This initiative is an important part of the *Beyond the Border* declaration, negotiated between Canada and the US. In 2011, as part of the *Beyond the Border Action Plan*, Canada committed to implementing a harmonized methodology for the screening of all air travellers. For CBSA, this involves the implementation of fully automated user managed scenario based rules. The API-PNR information is used to identify potential high

risk travellers.

→ Continue to Question 2

No

- 1.3 ☐ If there is no legal authority for the collection of personal information, it cannot be collected. Please consult your legal advisor to determine if there is authority to proceed with the program or activity.
****The PIA process must not continue without this key information.****

2. Necessity To Collect Personal Information

Is each element and sub-element of personal information collected or to be collected necessary to administer the program or activity?

Statutory reference: Section 4 of *Privacy Act*

Policy reference: Sections 6.1.1, 6.1.3, 6.1.4, 6.2.7 and 6.2.8 of *Directive on Privacy Practices*

YES

- 2.1 ☒ Ensure that all personal information necessary to administer the program or activity is listed in the relevant PIB.
- 2.2 ☒ AND, implement controls and procedures to ensure the CBSA does not collect more personal information than is necessary for the identified program or activity and that a continuing need exists for that information or its collection.
- Standards for API-PNR information elements are published by the World Customs Organization (WCO) and internationally recognized by other international governments, notwithstanding an individual country's privacy framework. The information received by the CBSA meets parameters set out in CBSA's regulations and does not use restricted information elements. Refer to the API-PNR Program PIA for the collection of API/PNR information.
 - Additionally, the Targeting Program continuously monitors and reports on the effectiveness of the targeting program relying on analytics, trend and patterns and operational intelligence for the effective use of scenarios which rely on API/PNR information.

2.3 Are secondary uses contemplated for the information collected?

☐ YES ☒ NO (Continue to Question 3)

2.3.2 If not, is there authority for the use or disclosure of the personal information?

☐ YES ☐ NO

→ Continue to Question 3

NO

- 2.3 ☐ Review the proposed elements and sub-elements of personal information outlined in "Section 3 – Analysis of Personal Information Elements" to identify those that are "necessary" and not merely useful. Document any changes.

3. Authority For the Collection, Use or Disclosure Of the Social Insurance Number*Is the collection of the Social Insurance Number (SIN) necessary to administer the program or activity?***Statutory reference:** Section 4 of *Privacy Act***Policy reference:** Section 6.2.13 of *Policy on Privacy Protection* and sections 6.1.1 and 6.2 to 6.4 of *Directive on Social Insurance Number***Also see** "Guidance for Preparing Information-Sharing agreements Involving Personal Information" and "Taking Privacy into Account Before making Contracting Decisions"**YES**

- 3.1 ☐ Collection of the SIN must be in compliance with the *Directive on Social Insurance Number* (please check all appropriate boxes below):

- 3.2 ☐ State legal authority for collecting the SIN:

OR, in the absence of a legal authority to collect the SIN:

- 3.3 ☐ Establish explicit authority through legislative amendment(s).
- 3.4 ☐ Establish legal authority as outlined in the *Directive on Social Insurance Number*.

AND, if disclosure of the SIN by the CBSA is to occur on a routine or systematic basis

- 3.4.1 ☐ to another federal institution that is authorized to collect it, or to another level of government, establish an agreement or arrangement that includes specific provisions to limit the use of the SIN.
- 3.4.2 ☐ to a contractor or other external service provider, establish a contract that includes specific provisions to limit the use of the SIN.
- 3.5 ☐ AND, ensure that the relevant **PIB** for the program or activity states the authority under which the SIN is collected and the purpose for which it is used.

→ Continue to Question 4

NO

- 3.6 ☒ The SIN is not necessary and it will not be collected, used or disclosed to administer the program or activity.

→ Continue to Question 4

4. Direct Collection - Notification and Consent (as appropriate)*Is personal information collected directly from the individual to whom it relates?***Statutory reference:** Sections 4 and 5 of *Privacy Act***Policy reference:** Sections 6.1.1, 6.2.6 and 6.2.9 to 6.2.13 of *Directive on Privacy Practices* and section 6.1.2 and 6.4.1 of *Directive on Social Insurance Number***YES**

- 4.1 ☐ A "Privacy Notice" (adapted for either verbal or written communications) must be provided to the individual at the time of collection and it must include the following elements:
- a) The purpose and authority for the collection
 - b) Any uses or disclosures that are consistent with the original purpose.
 - c) Any uses or disclosures that are not related to the original purpose
 - d) Any legal or administrative consequences for refusing to provide the personal information
 - e) That the "individual to whom the information relates" has rights of access to, correction of and protection of personal information under the *Privacy Act*.
 - f) A reference to the PIB for the program or activity
 - g) Why the SIN is collected, how it will be used and the consequence of not providing it.

AND, add a "Consent Statement" to the "Privacy Notice" as appropriate, if the personal information is to be used or disclosed for a purpose other than the original purpose (Secondary Use) or a consistent use, or, to authorize indirect collection of personal information.

- 4.2 ☐ The "Consent Statement" must include the following elements:
- a) The purpose of the consent and the specific personal information involved.
 - b) In the case of indirect collections, the sources that will be asked to provide the information.
 - c) Uses and disclosures that are not consistent with the original purpose of the collection and for which consent is being sought.
 - d) Any consequences that may result from withholding consent.
 - e) Any alternatives to providing consent
- 4.3 ☐ AND, implement controls and procedures to ensure that the CBSA keeps a record documenting whether or not an individual provided consent when it was sought, including a record documenting any withdrawal of consent when applicable.

Additional Consent Considerations (s. 77(1)(m) of the *Privacy Act*):

- ☐ Standards and mechanisms are in place to ensure that the individual has capacity to give consent.

→ Continue to Question 5

NO

- 4.4 ☒ The personal information necessary for the program or activity is not collected directly from the individual. It is collected indirectly, for example, from another program within the CBSA, or from another institution, government or third party.

→ Continue to Question 5

5. Indirect Collection - Consent or Authority Under Sec. 10 of Privacy Regulations

Is personal information collected indirectly from another source with the informed consent of the individual to whom it relates, or from a person authorized to act on behalf of the individual pursuant to section 10 of

the Privacy Regulations?

Statutory reference: Sections 4 and 5 of *Privacy Act* and section 10 of *Privacy Regulations*

Policy reference: Sections 6.1.1, 6.2.6 and 6.2.9 to 6.2.13 of *Directive on Privacy Practices* and sections 6.1.2 and 6.4.1 of the *Directive on Social Insurance Number*

YES

- 5.1 ☒ The notice and consent requirements stated at Question 4 apply. Please provide the "**Privacy Notice**" and/or "**Consent Statement**" below:

The SBT methodology relies on previously collected information through the existing API/PNR Program. Refer to the '*Privacy Act* Principle 3: Consent' section in the API/PNR Program PIA.

- 5.2 ☐ AND, implement controls and procedures to ensure the CBSA keeps a record documenting whether or not an individual provided consent when it was sought, including a record documenting any withdrawal of consent when applicable.

- 5.3 ☐ AND, if information is being collected from persons authorized to act on behalf of minors, incompetents or individuals who have been deceased for less than 20 years, implement appropriate mechanisms to ensure that such persons are authorized to act on behalf of individuals who do not have the capacity to provide consent.

→ Continue to Question 6

NO

- 5.4 ☐ → Continue to Question 6

6. Indirect Collection - Without Notification and Consent

Is personal information collected from another source without notice to or consent from the individual to whom the information relates?

Statutory reference: Sections 4, 5, 7 and 8 of *Privacy Act* and section 10 of *Privacy Regulations*

Policy reference: Sections 6.2.6 and 6.2.9 to 6.2.13 of *Directive on Privacy Practices*, section 6.2.15 of the *Policy on Privacy Protection* and sections 6.3.2 and 6.3.3 of *Directive on Privacy Impact Assessment*

YES

- 6.1 ☐ Where information is collected indirectly under any of the following circumstances without notice to, or consent from, the individual to whom it relates, please check the applicable boxes and explain as requested:

- ☐ a) The collection is a result of a disclosure to the CBSA under subsection 8(2) of the *Privacy Act*. State the applicable paragraph(s) of subsection 8(2) and provide a brief explanation for each:

Details:

- ☐ b) Direct notification of the individual might result in the collection of inaccurate information, or might defeat the purpose or prejudice the use for which the information is collected. Briefly explain why notice is not provided:

Details:

- ☐ c) The information involved in the program or activity is to be used solely for a non-administrative purpose in which no decisions are made about the individuals to whom the information relates.
- 6.2 ☐ AND, if any of the circumstances in a) b) or c) is applicable, ensure that it is reflected in the relevant **PIB**.
- 6.3 ☐ AND, if the information is to be used solely for a non-administrative purpose (box c above has been checked), ensure that the requirements under sections 6.3.2 and 6.3.3 of the *Directive on Privacy Impact Assessment* have been met, and that the decision of the official responsible for section 10 of the *Privacy Act* to proceed with a CBSA PIA for the program or activity has been adequately documented in the description of the program or activity in "*Section 1 - Overview and PIA Initiation*" of the CBSA PIA.
- 6.4 ☐ OR, if none of the circumstances in a) b) or c) is applicable, then the personal information must be collected directly from the individual, or indirectly with the consent of the individual. Please review the responses to Questions 4 and 5 and ensure that the "**Privacy Notice**" or the "**Consent Statement**" includes all of the required elements within [Question 4](#).
- Continue to Question 7

NO

- 6.5 ☒ All personal information is collected directly from the individual to whom it relates, or from another source with notice to, or consent from, the individual or a person authorized to act on behalf of the individual (see Questions 4 and 5 above). → Continue to Question 7

7. Retention and Disposal of Personal Information

Has Library and Archives Canada approved a records retention and disposal schedule that applies to the personal information?

Statutory reference: Section 12 of *Library and Archives Canada Act*, sections 6, 10 and 11 of *Privacy Act* and section 4 of *Privacy Regulations*

Policy reference: Sections 6.1.3, 6.2.11 to 6.2.13 and 6.2.23 of *Directive on Privacy Practices*

YES

- 7.1 ☒ Please identify the Record Disposition Authority (RDA) and describe the retention and disposal schedule:

Details: RDA Number: 90/00, as Per API/PNR PIB CBSA PPU 008

Retention and Disposal Standards: Records will be retained for 3.5 years from date of travel and then the records are destroyed. Where the API and PNR information relates to a person who is the subject of an investigation in Canada the API/PNR information will be transferred to an enforcement database of the Canada Border Services Agency (CBSA) and be retained in that system for a period of no more than 6 years and destroyed after 6 years.

- 7.2 ☒ AND, implement controls and procedures to ensure that personal information used to make a decision that directly affects an individual will be retained for a minimum of two years after the last

administrative action or, where a request for access to the information has been received, until such time as the individual has had the opportunity to exercise all his/her rights under the Act.

7.3 ☒ AND, if the CBSA intends to dispose of personal information that has been used for an administrative purpose prior to the expiration of the two-year minimum retention standard established by the *Privacy Regulations*, it must obtain the consent of the individual to whom the information relates before doing so.

7.4 ☒ AND, the CBSA must cite the RDA number, the retention period and the disposition standards for the personal information in the relevant PIB.

1. RDA Number 90/002. Records will be retained for 3.5 years from date of travel and then the records are destroyed. Where the API and PNR information relates to a person who is the subject of an investigation in Canada the API/PNR information will be transferred to an enforcement database of the CBSA and be retained in that system for a period of no more than 6 years and destroyed after 6 years. These details are cited in PIB CBSA PPU 008.

→ Continue to Question 8

NO

7.5 ☐ Provide a Records Disposition Submission to Library and Archives Canada describing the records containing the personal information for which the institution requires a RDA.

7.6 ☐ AND, obtain a RDA from Library and Archives Canada to allow the CBSA, under certain conditions, to dispose of records that no longer have operational utility for the program or activity.

7.7 ☐ AND, ensure that all the other applicable requirements listed under "YES" at Question 7 are met.

→ Continue to Question 8

8. Accuracy Of Personal Information

Will measures be adopted to ensure that personal information used by the CBSA for an administrative purpose is as accurate, up-to-date and complete as possible?

Statutory reference: Sections 6, 10 and 11 of *Privacy Act* and sections 10 and 11 of *Privacy Regulations*

Policy reference: Sections 6.1.1 and 6.2.9 to 6.2.16 of *Directive on Privacy Practices*

YES

8.1 ☒ Please check any of the following measures that will be adopted to ensure accuracy of the personal information and provide details as requested:

8.1.1 ☐ Personal information will be collected directly from the individual to whom it relates or it will be validated with the individual or a person authorized to act on behalf of the individual.

8.1.2 ☐ A data-matching process will be used to verify the accuracy of personal information against a "reliable source" (within or outside the CBSA) where this is authorized, or where consent was obtained.

Details:

8.1.3 ☒ In cases where direct collection or consent is not feasible, the CBSA will obtain information from

trusted sources (public or private) and verify accuracy against existing personal information before use.

Details: The personal information used by CBSA for the SBT is deemed to be accurate for the purposes it is used for based on the trusted source from which the information is obtained. Most of the personal information is derived from internal databases that have their own accuracy practices. This is also the case for external databases such as CPIC. In addition, when the traveller's information results in a match to a scenario, the Targeting Officer may use multiple trusted sources of information to validate the scenario results. As a result, the SBT process is in itself a measure to ensure that the personal information the Targeting Officer is using is as accurate as necessary for the purposes it is being used for.

- 8.1.4 ☐ Technological methods will be used to identify errors and discrepancies.

Details:

- 8.1.5 ☐ Other

Specify:

- 8.2 ☒ AND, if measures are adopted other than "*direct collection or validation with the individual or with a person authorized to act on behalf of the individual*", the CBSA must implement appropriate controls and procedures to ensure that:

- a) the technique(s) and the specific source(s) used to validate or update the personal information are documented;
- b) individuals are given the opportunity, whenever possible, to request correction of any inaccurate personal information before the information is used in a decision-making process that affects them;
- c) personal information can only be modified or corrected by those within the CBSA who have the authority to do so;
- d) when personal information is corrected or annotated, the record of personal information indicates the date of the last correction or annotation and the source of the information used to make the correction or annotation; and
- e) when personal information is corrected or annotated, other authorized holders of the information are notified about the correction or annotation and that all copies of the information in the possession of the CBSA are corrected / annotated.

Details:

Travellers have the right to request a copy of the API/PNR information that commercial carriers provide to the CBSA. They can also request that a notation be included if any of the information is incorrect as follows:

Pursuant to the *Privacy Act* and the *Access to Information Act*, the following can access their API/PNR records held by the CBSA:

- a) a Canadian citizen
- b) a permanent resident within the meaning of subsection 2 of the Immigration and

Refugee Protection Act

- c) A foreign national present in Canada
- d) A person present in Canada with the consent of the foreign national not present in Canada.

In addition, API/PNR program will afford access, correction and notation rights related to API/PNR information to persons that are not in Canada on an "informal basis". The disclosure request must be made to the CBSA using form BSF153, Travellers API/PNR Request, available on the CBSA website.

The capacity to change incorrect personal information contained in the systems exists, as noted in the *API/PNR Correction Process Flow*. The PAXIS IT Team of the Information Science and Technology Branch, Enforcement Systems Division, with the usage access level of Create Read Modify (CRM), is authorized to make these corrections and makes requested corrections in PAXIS as per the API/PNR Statement of Sensitivity (SOS) and the Threat and Risk Assessment (TRA).

- 8.3 ☐ AND, if appropriate, ensure that the "**Privacy Notice**" or "**Consent Statement**" and the relevant **PIB** are amended to identify the data-matching activity including the source(s).

→ Continue to Question 9

NO

- 8.4 ☐

Explain why such measures will not be adopted:

→ Continue to next Question 9

9. Use Of Personal Information

Will the personal information collected for the program or activity be used solely for the original purpose for which it was obtained or compiled, a use consistent with that purpose, or a purpose for which the information was disclosed to the institution pursuant to subsection 8(2) of the Privacy Act?

Statutory reference: Sections 5 and 7 to 11 of *Privacy Act*

Policy reference: Sections 6.1.1, 6.1.9, 6.2.9 to 6.2.13 and 6.2.17 of *Directive on Privacy Practices*, section 6.2.15 of *Policy on Privacy Protection* and Section IV of Appendix C of *Directive on Privacy Impact Assessment*

YES

- 9.1 ☒ Implement controls and procedures to ensure that access to the personal information for such purposes will be limited to authorized individuals who need to know the information to perform their official duties.

Details: Controls and procedures that deal with access to personal information are contained in the *Air Passenger Targeting Procedures*. For example, those procedures mandate that the Targeting Superintendent is responsible for monitoring the use of PAXIS to ensure compliance

with legislative requirements pertaining to the access, use, retention and disposal of API/PNR information. In addition, the *National Targeting Policy* contains substantive content related to controlling access to the content contained in the various systems used by Targeting Officers and other officials. Section 7 of the *Protection of Passenger Information Regulations* also contains content related to controlling access to personal information. Lastly, data masking rules per the EU Agreement have been incorporated into the PAXIS application limiting access to the API-PNR information.

- 9.2 ☒ AND, ensure that the "Data Flow Diagram" or "Data Flow Tables" completed for "Section 4 – Flow of Personal Information" of the CBSA PIA identify the areas, groups and individuals (e.g., the positions) within the CBSA who have a need-to-know to access to or handle the personal information, including their geographical location and where the personal information will be stored or retained.

Refer to Appendix A, API/PNR Authorized CBSA Officials and Access Level, CBSA D1-16-3 Memorandum.

- 9.3 ☐ AND, if the purposes for which the personal information is used includes any use(s) of the information for a non-administrative purpose, (such as research, statistical, audit and evaluation purposes) the CBSA will adhere to the requirements and principles in the **CBSA Privacy Protocol For Non-Administrative Purposes** (2012), in accordance with section 6.2.15 of the *Policy on Privacy Protection*, to address any impact that such non-administrative uses may have on privacy.

→ Continue to Question 10

Detail :

NO

- 9.4 ☐ Identify below any other uses of the personal information, in other words, any routine uses that are not directly related to the purpose of the collection, or, which are not consistent with that purpose or for which the information was disclosed to the CBSA pursuant to subsection 8(2) of the *Privacy Act*:

Detail :

- 9.5 ☐ AND, ensure that these other uses are reflected in the relevant PIB.

- 9.6 ☐ AND, include a description of these other uses in the "Privacy Notice" or "Consent Statement", as appropriate,

- ☐ AND, ensure the all the other applicable requirements listed under "YES" at Question 9 are met.

→ Continue to Question 10

10. Disclosures Directly Related to the Administration of the Program or Activity

Will personal information be disclosed for purposes directly related to the administration of the program or activity?

Statutory reference: Sections 5 and 8 to 11 of *Privacy Act*.

Policy reference: Sections 6.2.10, 6.2.11 and 6.2.13 of *Policy on Privacy Protection*, sections 6.2.1 to 6.2.3 of *Directive on Social Insurance Number*, sections 6.1.9, 6.2.9 to 6.2.13 and 6.2.15 to 6.2.20 of *Directive on Privacy Practices* and section IV of Appendix "C" of *Directive on Privacy Impact Assessment*)

Also see "Guidance for Preparing Information-Sharing agreements Involving Personal Information" and "Taking Privacy into Account Before making Contracting Decisions"

YES

- 10.1 ☒ Please check all applicable boxes below and, for each disclosure, identify the name of the organization or third party to which personal information will be disclosed. If it is disclosed within the CBSA, please identify the branch and the program or activity.

- 10.1.1 ☐ Within the CBSA for another program or activity

Detail: N/A

- 10.1.2 ☒ Other federal government institutions

Detail: Personal information associated with the results of SBT can be disclosed on a case by case basis to RCMP and/or CSIS. This process is not a new process caused by the application of SBT. This existed with risk scoring. Items 26-28 of the Memorandum D1-16-3 outlines the requirements for CBSA officials to track and maintain records of such disclosures.

- 10.1.3 ☐ Provincial, territorial or municipal governments institutions

Detail : N/A

- 10.1.4 ☒ Foreign government institutions and entities thereof

Detail: Limited personal information associated with the results of SBT is disclosed to the US CBP. This process is not a new process caused by the application of SBT. This existed with risk scoring.

The US CBP disclosure is addressed with the High-Risk Traveller Initiative (HRTI) PIA.

On March 9, 2005, Canada and the USA signed the Memorandum of Understanding for the Automated Exchange of Lookouts and the Exchange of Advance Passenger Information (API). In February 2008, the MOU was updated via an exchange of letters to initiate the sharing of Passenger Name Record information. In September 2009, the MOU was amended to update the targeting methodologies used by both countries. The MOU sets out the general principles and protections for the CBSA and USA CBP to share information on high-risk travellers destined to either country.

- 10.1.5 ☐ International organizations

Detail: N/A

10.1.6 ☐ The private sector (e.g., contractor or other external service provider)

Detail: N/A

10.1.7 ☐ Other

Detail: N/A

10.2 ☒ AND, ensure that:

- a) any such disclosure is made in compliance with section 8 of the *Privacy Act*, which allows disclosures of personal information with consent of the individual to whom the information relates (subsection 8(1)) or without consent in certain and limited circumstances pursuant to subsection 8(2) of the Act;
- b) only personal information elements that are necessary for the intended purpose are disclosed;
- c) the organization or third party receiving the personal information is authorized to do so;
- d) administrative, physical and technical safeguards appropriate to the sensitivity of the information will be applied to protect the information during and after its transmission (see Question 15);
- e) the organization or third party to which the personal information will be disclosed for the administration of the program or activity are identified in the "Consistent Use" section in the relevant **PIB** in *CBSA Info Source*, including the specific purpose of the disclosure; the "**Privacy Notice**" or "**Consent Statement**" describes any disclosures of information; and,
- f) the "Data Flow Diagram" or "Data Flow Tables" completed in "*Section 4 – Flow of Personal Information*" of the CBSA PIA include details on the disclosed personal information:

10.3 ☒ AND, any disclosure of personal information to another federal institution or outside the Government of Canada is governed by a formal agreement or arrangement (e.g., a Memorandum of Understanding, an accord, a contractual arrangement, etc.) to ensure that appropriate privacy protection clauses are included, and, where applicable, include provisions for inter-jurisdictional or transborder flows of personal information. Such clauses must cover the following topics:

- a) Control over personal information, where appropriate.
- b) Limitations on the collection, retention, use and disclosure of personal information.
- c) Measures (administrative, technical and physical) to protect the integrity and confidentiality of personal information.
- d) Measures governing the disposition of the personal information, where relevant
- e) Measures to ensure or verify that the personal information is only used for the purposes related to the agreement, arrangement or contract.
- f) Obligations are to be extended to other parties such as subcontractors.

→ Continue to Question 11

NO

- 10.4 ☐ There is no disclosure of personal information within or outside the institution for purposes that are directly related to the administration of the program or activity.

→ Continue to Question 11

11. Accounting For New Uses or Disclosures Not Reported in CBSA Info Source

Will controls and procedures be implemented to account for any new use or disclosure of the personal information that is not included in the relevant PIB published in CBSA Info Source?

Statutory reference: Sections 7 to 11 of Privacy Act and section 4 of Privacy Regulations

Policy reference: Sections 6.1.9 and 6.2.2 of Directive on Privacy Practices

YES

- 11.1 ☒ Appropriate controls and procedures have been or will be implemented to ensure that:
- a) the head of the institution (The ATI and Privacy Director) or the appropriate delegate is notified about any new use or disclosure of personal information that is not reflected in the PIB description published in *CBSA Info Source*;
 - b) the consent of the individual to whom the information relates is obtained in writing, as appropriate, prior to any new use of the information for an administrative purpose that is not reflected in the relevant PIB published in *CBSA Info Source*, unless the new use is considered to be consistent with the purpose for which the personal information was obtained or compiled and the Privacy Commissioner is notified, by the CBSA ATI and Privacy Director, forthwith regarding the new consistent use;
 - c) except as permitted under subsection 8(2) of the *Privacy Act*, any disclosure of personal information for a purpose that is not reflected in the relevant PIB published in *CBSA Info Source* will only be made with the consent of the individual to whom the information relates;
 - d) a record is kept for any new use or disclosure of personal information not described in the relevant PIB published in *CBSA Info Source*, and that this record is stored with the personal information to which it relates and retained for a minimum period of two years following such a use or disclosure;
 - e) if the information is disclosed to a federal investigative body under paragraph 8(2)(e) of the *Privacy Act*, the record of disclosure will be kept in a separate PIB for a period of two years where it will be available to the Privacy Commissioner for review upon request;
 - f) the Privacy Commissioner is notified, by the CBSA ATI and Privacy Director, forthwith, as required under subsection 9(4) of the Act, of any new use or disclosure that is consistent with the purpose for which the information was obtained or compiled, but which is not reflected in the relevant PIB published in *CBSA Info Source*;
 - g) the relevant PIB is amended in time for the next edition of *CBSA Info Source* to include any new use(s) or disclosure(s) that are consistent with the purpose for which the information was obtained or compiled, as well as any routine use(s) or disclosure(s) that do not fall within the categories of purpose of collection or consistent use and
 - h) the Privacy Commissioner is notified, by the ATI and Privacy Director, prior to or forthwith, as required under subsection 8(5) of the Act, about any disclosures made or to be made in the public interest or in the interest of the individual to whom the information relates.

i) Other

Detail: There are no new uses or disclosures of personal information contemplated in the change to SBT methodology.

→ Continue to Question 12

NO

11.2 ☐ Please explain why such controls and procedures will not be implemented

Detail:

→ Continue to Question 12

12. Safeguards - Statement Of Sensitivity

Has a Statement of Sensitivity (SoS) or similar analysis been completed to assess the degree of sensitivity of the personal information to be collected and retained for the program or activity?

Statutory reference: Sections 7 and 8 of Privacy Act.

Policy reference: Appendix C of *Directive on Privacy Impact Assessment* and sections 6.2.17 to 6.2.21 of *Directive on Privacy Practices, Policy on Government Security, Operational Security Standard: Management of Information Technology Security (MITS)*

YES

12.1 ☒ The information contained in the SoS or similar analysis has been taken into account when assessing the level of risks to privacy in "Section 2 - Risk Area Identification and Categorization" of the CBSA PIA.

→ Continue to Question 13

NO

12.2 ☐ Please explain why a SoS or similar analysis was not considered necessary to assess the sensitivity of the information.

Detail :

→ Continue to Question 13

13. Safeguards - Threat and Risk Assessment

Has a Threat and Risk Assessment (TRA) or a similar security assessment been completed for the program or activity? (Input to this section must be coordinated with and reviewed by CBSA – IT - Security Directorate)

Statutory reference: Sections 7 and 8 of Privacy Act.

Policy reference: Appendix C of *Directive on Privacy Impact Assessment* and sections 6.2.17 to 6.2.21 of *Directive on Privacy Practices, Policy on Government Security, Operational Security Standard: Management of*

*Information Technology Security (MITS)***YES**

- 13.1 ☒ Reference the title of the TRA or other security assessment in "Section 6 – Supplementary Documents List" and provide a brief synopsis of the assessment in the space below:

Detail: Several TRA's have been undertaken over the years that were focussed on PAXIS and an IT Security Risk Mitigation Analysis was conducted in 2013. It was focused on Scenario Based Targeting for High Risk Travellers – Transition Architecture R1 & R2. This document characterized the related information as Protected B with a medium integrity risk and availability risk. It also indicated that there were no unmet security obligations. Because the change from risk scoring to SBT was not considered substantive from the perspective of CBSA IT security officials, this also contributed to the decision to not carry out a full TRA.

- 13.2 ☒ AND, obtain assurances from the officials responsible for the program or activity that the measures recommended in the assessment have been implemented to ensure the confidentiality, availability and integrity of the personal information.
- 13.3 ☒ AND, ensure that any residual risks to personal information are known and accepted by the executive or senior official responsible for the program or activity and the Head or delegated authority for the *Privacy Act*. (ATI and Privacy Director)

→ Continue to Question 14

NO

- 13.4 ☐ If a TRA or similar security assessment is underway, simply reference that fact in the space below and indicate when it is likely to be completed. If there is no intent to complete one, please explain.

Detail :

→ Continue to Question 14

14. Safeguards - Administrative, Physical and Technical

Please identify below any administrative, physical and technical safeguards in place, or to be implemented, for this program or activity to ensure the confidentiality, availability and integrity of the personal information.

Statutory reference: Sections 7 and 8 of *Privacy Act*

Policy reference: Appendix C of *Directive on Privacy Impact Assessment* and sections 6.2.17 to 6.2.21 of *Directive on Privacy Practices, Policy on Government Security, Operational Security Standard: Management of Information Technology Security (MITS)*

Please check all that apply, including safeguards identified by the TRA or similar security assessment.

14.1 Administrative safeguards

- ☒ Internal security and privacy policies and procedures
- ☒ Staff training on privacy and the protection of personal information
- ☒ Screening and security checks of employees

- ☒ Appropriate security levels for employees who will have access to personal information
- ☒ Contingency plans and documented procedures in place to identify and respond to security and privacy breaches, and to communicate security violations to the data subject, law enforcement authorities and relevant program managers
- ☒ Regular monitoring of users' security practices
- ☒ Methods to ensure that only authorized personnel who need to know have access to personal information
- ☐ Other

Detail :

14.2 Physical safeguards

- ☒ Restricted access areas
- ☒ Security guards
- ☒ Identification badges are worn by staff at all times
- ☒ After hours alarms and monitoring systems
- ☒ Locked filing cabinets
- ☒ Combination locks
- ☒ Safes
- ☐ Cipher locks
- ☒ Key cards
- ☒ Video surveillance (closed-circuit television)
- ☒ Secured server locations
- ☒ Backups secured off-site
- ☐ Other

Detail:

14.3 Technical safeguards

- ☒ Role-based user authorization and authentication
- ☐ Biometrics
- ☒ Passwords (minimum of 6 characters long, include alpha and numeric characters)
- ☒ Passwords are changed by users every 90 days and recently used passwords cannot be re-used)
- ☒ Password protected screensavers
- ☒ Session-time out security (automatically locks an account after a session has been idle for a specified amount of time)
- ☒ Firewalls
- ☒ Intrusion Detection System (IDS)
- ☐ Virtual Private Network (VPN)

- ☒ Encryption of sensitive information
- ☒ Government of Canada Public Key Infrastructure Certificates (PKI)
- ☐ External Certificate Authority (CA)
- ☒ Audit trails
- ☐ Other

Detail :

→ Continue to Question 15

15. Technology and Privacy - Tracking Technologies

Will the information system(s) used to deliver the program or activity employ cookies or other tracking technologies to collect personal information about users and their transactions?

Statutory reference: Sections 4 to 10 of the *Privacy Act* and section 4 of *Privacy Regulations*

Policy reference: Subsections 6.1.1, 6.1.3, 6.1.9, 6.2.9 to 6.2.13, 6.2.17 and 6.2.23 of *Directive on Privacy Practices*

YES

- 15.1 ☐ The specific tracking technologies to be used is adequately described under Part 6: Technology and Privacy of "Section 2 – Risk Area Identification and Categorization" of the CBSA PIA;
- 15.2 ☐ AND, the collection of any personal information using such technologies is reflected in the relevant *PIB* and in "Section 3 – Analysis of Personal Information Elements" of the CBSA PIA;
- 15.3 ☐ AND, the use of such technologies to collect information about users and their transactions is adequately reflected in the "Privacy Notice";
- 15.4 ☐ AND, those responsible for implementing and using tracking technologies to collect personal information or who may have access to personal information collected through these methods are made aware of privacy and security policy requirements;
- 15.5 ☐ AND, where personal information collected through such tracking technologies is used to make a decision that directly affects the individual to whom the information relates, it will be retained for a minimum of two years after the last administrative action as required under the *Privacy Regulations*.

→ Continue to Question 16

NO

- 15.6 ☒ Tracking technologies are not used to collect personal information about users.

→ Continue to Question 16

16. Technology and Privacy - Surveillance or Monitoring

Will the new or modified program or activity result in new or increased surveillance or monitoring of a targeted population?

Statutory reference: Sections 4 to 10 of *Privacy Act*, section 4 of *Privacy Regulations* and section 8 of the

Charter of Rights and Freedoms

Policy reference: Subsections 6.1.1, 6.1.9, 6.2.9 to 6.2.13 and 6.2.17 of *Directive on Privacy Practices*

YES

- 16.1 ☐ Consult with your legal advisors to determine whether or not such surveillance or monitoring activities raise any issues relating to the *Charter of Rights and Freedoms*, the *Privacy Act* or other applicable acts.
- 16.2 ☐ And, ensure the surveillance or monitoring method(s) to be used, the characteristic(s) of the targeted population and the scope of the surveillance or monitoring are adequately described under Part 6: Technology and Privacy of "*Section 2 – Risk Area Identification and Categorization*" of the CBSA PIA.
- 16.3 ☐ AND, any personal information collected or created as a result of such surveillance or monitoring is described in the relevant PIB and in *Section 3 – Analysis of Personal Information Elements* of the CBSA PIA.
- 16.4 ☐ AND, the collection or use of personal information through surveillance or monitoring is adequately reflected in the "**Privacy Notice**", unless such notification might result in the collection of inaccurate information or defeat the purpose or prejudice the use for which the personal information is collected.
- ☐ If notice about surveillance or monitoring will not be provided

Detail explain why:

- 16.5 ☐ AND, those responsible for implementing and using such surveillance or monitoring method(s) or who may have access to personal information collected or created through these methods are made aware of privacy and security policy requirements.

→ Continue to Question 17

NO

- 16.6 ☒ The new or modified program or activity will not result in surveillance or monitoring.

→ Continue to Question 17

17. Considerations Related to Compliance, Regulatory Investigation, Enforcement

Does the program or activity involve compliance/regulatory investigation or law enforcement, surveillance or intelligence gathering that targets specific individuals against whom penalties, criminal charges or sanctions may be applicable?

Statutory reference: Sections 4 to 10 of *Privacy Act*, section 4 of *Privacy Regulations* and section 8 of the *Charter of Rights and Freedoms*

Policy reference: Subsections 6.1.1, 6.1.9, 6.2.9 to 6.2.13 and 6.2.17 of *Directive on Privacy Practices*

YES

- 17.1 ☒ Consult with your legal advisors to determine whether or not the compliance/regulatory investigation or law enforcement activities raise any issues relating to the *Charter of Rights and Freedoms*, the *Privacy Act* or other applicable acts.

- 17.2 ☒ AND, identify the legislative authority and the specific regulatory or law enforcement purpose involved:

Detail : The authority to collect personal information is authorized by section 107.1 of the Customs Act, and the Passenger Information (Customs) Regulations, paragraph 148(1)(d) of the Immigration and Refugee Protection Act and regulation 269 of the Immigration and Refugee Protection Regulations.

- 17.3 ☒ AND, if the legislative authority differs from the legal authority for the program or activity, ensure it is adequately reflected in the response to Question 1 of "Section 5 – Privacy Compliance Analysis" and in "Section 1 – Overview and PIA Initiation" of the CBSA PIA.
- 17.4 ☒ AND, any personal information collected or created as a result of such regulatory or criminal enforcement, surveillance or intelligence gathering program or activity is described in the relevant PIB and in "Section 3 – Analysis of Personal Information Elements" of the CBSA PIA.
- 17.5 ☒ AND, the collection or use of personal information through these compliance / regulatory investigation or enforcement activities is adequately reflected in the "Privacy Notice", unless such notification might result in the collection of inaccurate information or defeat the purpose, or prejudice the use, for which the personal information is collected.
- ☐ If notice about the compliance/regulatory investigation or law enforcement activities will not be provided.

Details explain why: N/A

NO

- 17.6 ☐ The program or activity does not involve the conduct of regulatory or criminal enforcement, surveillance or intelligence gathering.

SECTION 6 - Summary of Analysis and Recommendations

This table summarizes the privacy risks identified through the PIA process, and categorizes risk levels as low, moderate or high. Risks are expressed in terms of both likelihood of the risk occurring and the impact should it occur. The goal of privacy risk management is to identify and maintain privacy risks within acceptable bounds. The higher ratings provide an indication of priority areas for implementing suggested risk mitigation mechanisms or strategies. This report identifies a number of privacy risks and the measures recommended mitigating or eliminating these risks.

Criteria for ranking are set as follows:

- Low: There is a remote possibility that the risk will materialize and/or the impact of the risk to the program is minor.
- Moderate: The possibility of the risk materializing is very low although the impact of such a risk is high, OR the possibility of the risk materializing is high but the impact of such a risk is minor, OR the impact and likelihood of the risk occurring are both determined to be moderate.
- High: There is a near certainty that the risk will materialize if no corrective measures are taken and/or the impact of the risk on the program is severe.

Element	Nature of risk	Level of risk			Mitigating Mechanism
		Low	Mod	High	
Openness	The API/PNR Program PIB does not reflect the use of SBT methodology nor does it fully reflect statutory authority for use of the personal information	✓			When timely, the API/PNR Program PIB should be updated to reflect the change from risk scoring to SBT and to more fully reflect the statutory authority for the use of the personal information.

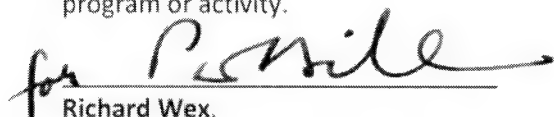
SECTION 7 - SUPPLEMENTARY DOCUMENTS LIST [TBC]

Document	Document Reference	PIA Reference
<i>Beyond the Border Action Plan</i>	http://actionplan.gc.ca/en/page/bbg-tpf/beyond-border-action-plan Establishing a common approach to screening travellers	Executive Summary Section 1: Summary of the project, initiative, or change Section 5.1 Legal Authority
<i>Immigration and Refugee Protection Act</i>	http://laws.justice.gc.ca/en/I-2.5/	p.6 Exec Summary Section 1 Legal Authority Section 5.1 Legal Authority
<i>Section 7.1 and Section 107.1 of the Customs Act</i>	http://laws-lois.justice.gc.ca/eng/acts/C-52.6/page-5.html#h-11 http://laws-lois.justice.gc.ca/eng/acts/C-52.6/page-69.html#h-7	p.6 Exec Summary Section 1 Legal Authority Section 5.1 Legal Authority
<i>Passenger Information (Customs) Regulations</i>	http://laws-lois.justice.gc.ca/eng/regulations/SOR-2003-219/FullText.html	p.6 Exec Summary Section 1 Legal Authority Section 5.1 Legal Authority
<i>Protection of Passenger Information Regulations</i>	http://laws.justice.gc.ca/eng/SOR-2005-346/page-1.html	p.6 Exec Summary Section 1 Legal Authority Section 4.4 External Use and Disclosure Section 5.1 Legal Authority Section 9.1 Use of Personal Information
<i>Section 269, Immigration and Refugee Protection Regulations</i>	http://laws-lois.justice.gc.ca/eng/regulations/SOR-2002-227/FullText.html#h-121	p.6 Exec Summary Section 1 Legal Authority Section 5.1 Legal Authority
<i>SBT IT Security Risk Mitigation Analysis (IRMA)</i>	Provided	Section 2 Beyond the Border Privacy Principles Section 13 Safeguards – Threat and Risk Assessment
<i>CBSA Security Policy</i>	http://atlas/cb-dgc/pol/cm-mc/sv-vs/index_eng.asp	Section 2 Personal Information Transmission
<i>US CBP Memoranda of Understanding for the Automated Exchange of Lookouts and the Exchange of Advance Passenger Information (API)*</i>	Provided	Section 2 Program or Activity Partners Section 3 Other Databases Section 10.1.4 Disclosures-Foreign Government Institutions
<i>Advance Passenger Information/Passenger Name Record (API/PNR) Project PIA Report, June 12, 2003</i>	Provided	Executive Summary Section 1 Scope of this PIA Section 2 Beyond the Border Privacy Principles
<i>High Risk Traveller Identification Initiative Privacy Impact Assessment, March 29, 2004</i>	Provided	Executive Summary Section 1 Scope of this PIA Section 4 Data Flow-Description
<i>Memorandum of Understanding between the Canadian Police Information Centre (CPI) a</i>	This MOU sets out the roles and responsibilities of the Parties in regards to the provision of access to	Section 3 Other Databases Section 4.2 Data Flow Model-Table

<i>National Police Service of the Royal Canadian Mounted Police and the Canada Border Services Agency, Borders Intelligence Division (Regional Intelligence Officers) & Immigration Warrant Response Center, September 29, 2007</i>	designated agency employees to the CPIC databases	
<i>Memorandum of Understanding Between Citizenship & Immigration Canada and the Canada Border Services Agency (2011) Information Sharing Annex 2012</i>		Section 3 Other Databases Section 4.2 Data Flow Model-Table
<i>CBSA Memorandum D1-16-3 Administrative Guidelines for the Provision to Others, Allowing Access to Others and Use of Advance Passenger Information (API) and Passenger Name Record (PNR) Data</i>	Provided	Section 2 Personal Information Transmission Section 4.2 Data Flow Model-Table Section 4.6 Other Possible Considerations-Access Section 9.2 Use of Personal Information Section 10.1.2 Disclosures-Other Federal Gov't Institutions
<i>Policy Guidelines on the Disclosure of Customs Information</i>	http://www.cbsa-asfc.gc.ca/publications/pub/bsf5150-eng.html	Section 2 Personal Information Transmission

SECTION 8 - FORMAL APPROVAL

The following signature represents a commitment to comply with sections 4 to 8 of the *Privacy Act* and the related privacy policy requirements outlined in the CBSA PIA as they relate to the administration of the identified program or activity.


Richard Wex,
Vice-President, Programs Branch

Dec 27, 2013.

Date

Note: Responsibility for sections 4 to 8 of the *Privacy Act* rests with all employees of government institutions that handle personal information. Officials who manage such programs and activities are responsible for ensuring that such requirements are implemented as part of the administration of the program or activity.

The following signature represents a commitment by the Head of the institution or his/her delegate(s) who is responsible for establishing personal information banks in accordance with section 10 of the *Privacy Act*.


Dan Proulx,
Director, Access to Information and Privacy

DEC 18 2013

Date

Note: Under the *Privacy Act*, the Head or his/her delegate(s) is responsible for complying with legal and relevant privacy policy requirements related to the approval and registration of personal information banks

Annex A: Privacy Compliance Checklist and Other Considerations

Privacy Compliance Analysis question #	Action required to support legal and policy compliance (cross reference to relevant question of <i>Section 5 – Privacy Compliance Analysis</i>)	Done	To be done
1	Legal authority for the program or activity has been established and is reflected in the relevant PIB.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2	a) The categories and elements of personal information to be collected for the new program or activity have been carefully assessed based, for example, on the CBSA's experience gained with the administration of a similar program or activity. The personal data collected will be limited to only that which is required.) b) Categories and elements of personal information have been described in the relevant PIB for the program or activity. c) Controls and procedures will be implemented to ensure the CBSA does not collect more personal information than necessary for the program or activity and that a continuing need exists for the personal information and its collection.	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
4 and 5	a) All of the requisite "Privacy Notices" and "Consent Statements" that meet the requirements of sections 6.2.9 to 6.2.12 of the <i>Directive on Privacy Practices</i> have been drafted. (Texts of the notices and consent statements must be included as an annex.) b) Controls and procedures have been implemented to keep records of individual consents, and to ensure that persons acting on behalf of individuals who do not have the capacity to provide consent have the authority to do so under section 10 of the <i>Privacy Regulations</i> .	<input type="checkbox"/> <input type="checkbox"/>	<input checked="" type="checkbox"/> <input type="checkbox"/>
7	a) A Records Disposal Authority (RDA) has been approved by Library and Archives Canada to authorize the disposal of the records containing personal information for the program. b) Controls and procedures have been implemented within the program or activity and the CBSA ATI and Privacy Division to ensure that information that has been used for an administrative purpose will be kept for the minimum retention period established by the Privacy Regulations. c) Reference to the RDA, the retention period and the disposition standards for the program have been cited in the relevant PIB.	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

Privacy Compliance Analysis question #	Action required to support legal and policy compliance (cross reference to relevant question of Section 5 – Privacy Compliance Analysis)	Done	To be done
8	Controls and procedures are in the process of being implemented to ensure that the personal information associated with the program is as accurate, complete and up-to-date as necessary.	<input checked="" type="checkbox"/>	<input type="checkbox"/>

**Other Privacy Considerations related to specific principles that are not explored in the previous 17 sections:
 (these considerations should be explored in the Executive Summary)**

Openness	Describe how the results of any privacy impact assessment or audit will be made available to the public. The Executive Summary will be published on the external CBSA ATI and Privacy Division website at http://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/pia-efvp/atip-aiprp/pias-sefp-eng.html	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Are policies and practices relating to the proposal's management and handling of personal information available to the public?	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Is there a communications plan to explain to the public how personal information will be managed and protected?	<input type="checkbox"/>	<input type="checkbox"/>
	Is there a clearly defined and easy process for individuals to access such information and/or communicate with appropriate individuals with respect to policies and practices relating to management and protection of personal information?	<input type="checkbox"/>	<input type="checkbox"/>
	Where appropriate, will public consultation take place on the privacy implications of the proposal?	<input type="checkbox"/>	<input type="checkbox"/>
Individual's Access to Personal Information	Is the system designed to ensure that an individual can have access to his/her personal information, including all other programs or applications that have received copies of the information? s. 12(1)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Are there documented procedures developed or planned on how to make privacy requests or requests for the correction of personal information? s. 12 (2)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Are individuals provided with access to their personal information in the official language of their choice? s. 17(2)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	If appropriate, are individuals provided with access to their personal information in an alternative format? s. 17(3)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Challenging	Are the complaint procedures for the proposed program or service	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Privacy Compliance Analysis question #	Action required to support legal and policy compliance (cross reference to relevant question of <i>Section 5 – Privacy Compliance Analysis</i>)	Done	To be done
Compliance	consistent with legislated requirements? s. 29-35		
	To improve information management practices and standards, has a procedure been established to log and periodically review the nature, frequency and resolution of complaints?	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Are there oversight and review mechanisms implemented or available to ensure accountability?	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Have oversight agencies, including the Office of the Privacy Commissioner, issued reports or opinions on issues that would be relevant to the proposal?	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Annex B: Office of the Privacy Commissioner Expectations

In their March 2011 document, *Expectations: A Guide for Submitting Privacy Impact Assessments* to the Office of the Privacy Commissioner of Canada, the Office of the Privacy Commissioner (OPC) has expressed the importance of analysing the risks of the project, program or initiative against the ten universal privacy and fair information practice principles of the Canadian Standards Association Model Code for the Protection of Personal Information.

The most relevant demonstration of the privacy risk and compliance analysis is the action plan. The OPC has said the following in their **Expectations** guide with respect to the action plan:

Once privacy risks and their proposed mitigating measures have been identified, we expect to see an Action Plan drawn up by the institution, indicating a specific time frame for remedying or mitigating the risks that have been identified, and if possible, naming a specific person or staff position accountable for taking action.

The action plan must list all privacy risks and compliance issues identified in the PIA and supplementary documentation. All risks and issues must be organized by the 10 universal privacy principles.

All recommendations and proposed mitigation strategies must also be described in the action plan. Identify the responsible program area and the timeline for completion or implementation of the strategy. The ATI and Privacy Division will provide programs with an action plan template to be addressed near the end of the PIA process.

The expectations of the OPC for each privacy principles are included below for your reference.

Accountability

Under this principle the OPC would expect to see documentation of an administrative structure for privacy, including input from legal services, access to information and privacy and information technology branches within an institution, with defined processes for determining when new projects require PIAs, for carrying them out, implementing mitigating measures and auditing for assurance of compliance. We expect PIA reports to be signed off at the appropriate level, and that training in privacy issues and procedures has been documented and is refreshed with employees regularly; and that privacy protective language is included in all contracts with third parties handling personal information in accordance with TBS guidance documents and internationally accepted best practices; and that regularly scheduled privacy compliance audits will be undertaken and the findings acted upon.

Identifying Purposes

The Privacy Act restricts federal government institutions to the collection of personal information that relates directly to an operating program or activity of the institution, so we would expect to see a clear description of the program and why each piece of information is needed; a description of the legislative authority for the collection; a clear listing of all the data elements collected; copies of any relevant documents such as application forms identifying the purpose for the collection or on-line notices of use; a copy of an up to date Personal Information Bank (PIB) description; a statement of any proposed new consistent use of information previously collected and a clear rationale as to how the use is reasonable

and directly connected to the original collection -- this may include an analysis of how an individual to whom it relates would reasonably expect it to be used for that purpose; a statement outlining any intended secondary uses of the information; whether the information is collected directly from the individual and if not, why; and a description of how personal information used for planning, forecasting or statistical purposes would be anonymized or de-linked from individual identifying information.

Consent

This is closely tied to the Identifying Purpose principle. Under this principle, OPC would expect to see a copy of notification language on forms or websites; a clear description of the purpose for collection; a rationale for not seeking consent, as is provided for in the Privacy Act; for web sites, a copy of the Privacy Notice Statement under which personal information is submitted to the institution.

Limiting Collection

Under this principle, OPC would expect to see a clear justification of the need for each data element collected, in keeping with the requirement of the Privacy Act that no personal information is to be collected by a government institution unless it relates directly to an operating program or activity of the institution; an indication that a data minimization exercise has been undertaken to ensure that each data element is necessary and that this exercise will be refreshed regularly; and that information collected from another department for a secondary use will be purged of all but the essential data elements before use.

Limiting Use, Disclosure and Retention

Under this principle, OPC would expect to see a description of the specific uses and proposed disclosures of the information; a clear statement limiting the use of the information to the purposes identified; a clear retention policy and disposition schedule that is also noted in the PIB; a process for destruction of the information that is in keeping with the Privacy Act and Regulations; copies of MOUs or agreements with third parties to whom information is disclosed governing its use, retention and disclosure, and clauses with contractors or sub-processors of information indicating the originating institution has the right to audit for compliance with privacy provisions.

Accuracy

Under this principle, OPC would expect to see a description of the process used by entities to ensure accuracy, particularly when administrative decisions are made; a description of how changes to records are logged and monitored; a statement of whether automated decision-making based on risk profiles is being undertaken and how automated decisions are vetted for accuracy; an explanation of the processes open to individuals seeking to correct information; a description of the process by which second or third parties to whom information has been disclosed will be notified of changes and corrections to the record; and a description of how audit trails of records transactions are monitored and evaluated.

Safeguards

OPC would expect to see under this principle a description of the physical and electronic safeguards that are in place to protect information; a Threat & Risk Assessment (TRA) with emphasis on privacy risks and concerns and a discussion of how these concerns have been remedied or addressed; a notation that encryption is used for personal information both in transit and at rest; a description of how system logs of information transactions are monitored for inappropriate use, including viewing of the information;

strong electronic access control, including controls on remote access, and the use of mobile devices; policies for the use of portable storage devices such as flash drives; a description of role-based access controls; and a description of the steps taken to ensure complete destruction of the information at the end of its life cycle.

Openness

Under this principle, OPC would expect to see a summary of the PIA written in plain, understandable language, posted on the institutional website in a manner accessible to the general public and containing a link to the relevant PIB description in CBSA Info Source; for particularly sensitive or privacy invasive programs we would expect to see the public communications plan described in the PIA, including a variety of methods such as posters, brochures and media announcements as well as detailed discussion of the PIA in the institution's Annual Report under the Privacy Act; a description of consultations with key stakeholders and the privacy risks or concerns raised should be readily available on the website; the name and contact information of an individual accountable for the handling of personal information should be easily obtained through the website or by calling the institution's main public number.

Individual Access

Under this principle, OPC would expect the PIA to include a description of any informal process the CBSA may have in place for access to and correction of personal information; an up to date and comprehensive description of information contained in the PIB corresponding to the initiative; a description of the process by which information in the hands of third parties is corrected following requests; a description of how the general public is made aware of these processes, for example, by a link and/or a toll-free number shown on the home page of the institutional website.

Challenging Compliance

OPC would expect to see the PIA address this principle by indicating clearly who is responsible for receiving and resolving privacy complaints; describing complaints that may have been received in any similar activity or pilot project and how they were handled; including privacy issues in project evaluations or feasibility reports; describing how and when compliance audits for privacy will be undertaken; including information on how to file a complaint with OPC under the Privacy Act; and reporting in some detail on specific and/or systemic privacy issues in its Annual Reports.

Annex C: Categories of Personal Information

The **Description** section in a personal information bank (PIB) describes the personal information in the records to which the bank relates. Treasury Board Secretariat has established the following categories of personal information, which give examples of specific elements of personal information that fall under each category. The purpose of the categories is to reduce the number of personal information elements that need to be listed in the Description section. These categories are representative of the personal information collected by most institutions, and they now appear in many of the CBSA registered PIBs. The ATI and Privacy Division modified the original list to reflect CBSA business lines.

- Biographical information (e.g. work history, curriculum vitae, family information, Passenger Information, etc.)
- Biometric information (e.g. blood type, eye or facial scan, DNA, finger / hand prints, etc.)
- Contact information (e.g. work and / or home information, including postal and e-mail addresses, telephone, fax, cell phone numbers, etc.)
- Citizenship status or Nationality (e.g. citizen, landed immigrant, etc.)
- Crew detailed information
- Criminal checks / history (e.g. information related to criminal record checks, investigations, charges, conviction dates and locations, pardons, etc.)
- Date of birth
- Date of death
- Destination City
- Employee identification number (e.g. Personal Record Identifier)
- Employee personnel information (e.g. records of attendance and leave, notices of disciplinary action, alternative work arrangements, decisions concerning compensation and fitness for work, official languages qualifications, salary, deductions, level of security clearance, performance reviews and appraisals, rating board assessments, including evaluation notes from staffing boards, training and development course applications and evaluations, etc.)
- E-Ticket Information
- Financial information (e.g. income, investments, mortgages, loans, orders of garnishment, financial institution information for direct deposit and other banking purposes, including name and branch number of institution, account number(s) and name(s) on accounts, etc.)
- FOSS Case Number
- Gender
- Itinerary Cities
- Language (e.g. mother tongue, official and other languages, etc.)
- Medical information (e.g. psychological assessments, blood type, etc.)
- Name (e.g. last name (surname/family name), given names (first, second or more), maiden name, nicknames, aliases, etc.)
- Opinion or views of, or about, individuals
- Passenger Name
- Passport Number or Travel Document Number

Place of ticket purchase

Photos

Physical attributes (e.g. height, weight, color of hair and eyes, physical markings (scars, tattoos, body piercing), etc.)

Place of birth

Place of death

Port of Embarkation and Port of Debarkation

Signature

Special Travelling Considerations such as Employee Pass, Buddy Pass and Parental Passes

Visa Number



Primary Inspection Kiosk (PIK) Implementation 1.0

Privacy Impact Assessment (PIA)

Passenger Processing Unit
Traveller Transformation – Air Mode Division
Programs Branch



Version Control

Version	Author	Action	Date
1	Yvonne Robinson	Initial Draft	May 2016
2	Marnie McKinstry	Review and comment	June 2016
3	Wendy Luciani	Review and submit to ATIP	July 2016
4	Wendy Luciani	Revise to address ATIP feedback	August 2016
5	Suhaila Haji	Revise to address ATIP feedback	November 2016
6	Suhaila Haji	Revise to address ATIP feedback	December 2016
Final	Wendy Luciani	Copy for approval	December 2016
	Suhaila Haji	Revise to address ATIP feedback	December 2016
	Wendy Luciani	Copy for approval	January 2016

Stakeholders

Name	Role	Contact Information
Yvonne Robinson	PIA Consultant	
Brigitte Chouinard	Program Officer	Brigitte.Chouinard@cbsa-asfc.gc.ca 343-291-5601
Wendy Luciani	A/Manager	Wendy.Luciani@cbsa-asfc.gc.ca 343-291-6899
Marie Lallier	Senior Project Manager, Statistics Canada	marie.lallier@canada.ca 613-951-4967
Robin Lortie	A/Manager, Corporate Affairs Branch	Robin.lortie@cbsa-asfc.gc.ca 343-291-6897
Adam Norwick	Senior Policy Officer, ATIP	Adam.Norwick@cbsa-asfc.gc.ca 343-291-6985
Jill Bausch	Senior Privacy Policy Officer, Employment and Social Development Canada	Jill.Bauch@hrsdc-rhdcc.gc.ca 819-654-7025
Maha Loubani	Information Management Analyst	Maha.Loubani@cbsa-asfc.gc.ca
Nelson Montgomery	A/Senior Program Advisor	Nelson.Montgomery@cbsa-asfc.gc.ca 343-291-5596
Suhaila Haji	Senior Program Advisor	Suhaila.Haji@cbsa-asfc.gc.ca 343-291-5594
Maureen Haley	A/Manager	Maureen.Haley@cbsa-asfc.gc.ca 613-957-6014
Steve Whittaker	Manager, Risk Assessment and Consultation	Steve.Whittaker@cbsa-asfc.gc.ca 343-291-6916

Table of Contents

VERSION CONTROL	2
STAKEHOLDERS	2
EXECUTIVE SUMMARY	6
ABBREVIATIONS AND ACRONYMS	8
DEFINITIONS	10
SECTION 1 - OVERVIEW AND INITIATION	11
SECTION 2 - RISK AREA IDENTIFICATION AND CATEGORIZATION	20
Type of Program or Activity	20
Type of Personal Information Involved and Context	23
Program or Activity Partners and Private Sector Involvement	25
Duration of the Program or Activity	25
Program Population	26
Technology and Privacy	26
Personal Information Transmission	27
Risk Impact to the CBSA	28
Risk Impact to the Individual or Employee	29
SECTION 3 - ANALYSIS OF PERSONAL INFORMATION ELEMENTS	30
SECTION 4 - FLOW OF PERSONAL INFORMATION	34
4.1 Data Flow Model - Diagram	34
4.3 Internal Use and Disclosure	46
4.4 External Use and Disclosure	47
4.5 Retention / Storage	50
4.6 Other Possible Considerations	50
SECTION 5 - PRIVACY COMPLIANCE ANALYSIS	51
1. Legal Authority for Collection of Personal Information	51
2. Necessity to Collect Personal Information	52
3. Authority for the Collection, Use or Disclosure of the Social Insurance Number	53
4. Direct Collection - Notification and Consent (as appropriate)	54
5. Indirect Collection - Consent or Authority under Sec. 10 of Privacy Regulations	55
6. Indirect Collection - Without Notification and Consent	56
7. Retention and Disposal of Personal Information	57
8. Accuracy of Personal Information	58
9. Use of Personal Information	59
10. Disclosures Directly Related to the Administration of the Program or Activity	60
11. Accounting for New Uses or Disclosures Not Reported in CBSA Info Source	63
12. Safeguards - Statement of Sensitivity	63
13. Safeguards - Threat and Risk Assessment	64
14. Safeguards - Administrative, Physical and Technical	65
15. Technology and Privacy - Tracking Technologies	66
16. Technology and Privacy - Surveillance or Monitoring	67
17. Considerations Related to Compliance, Regulatory Investigation, Enforcement ..	67
SECTION 6 - SUMMARY OF ANALYSIS AND RECOMMENDATIONS	70

SECTION 7 - SUPPLEMENTARY DOCUMENTS LIST	75
SECTION 8 - FORMAL APPROVAL	76
ANNEX A: PRIVACY COMPLIANCE CHECKLIST AND OTHER CONSIDERATIONS.....	77

Privacy Impact Assessment Date / Version:	YYYY-MM-DD (Date sent to OPC)
Office of the Privacy Commissioner file #:	PIA # 000415-A
Project Implementation Plan (if applicable)	2017-03-07
Federal Institution:	Canada Border Services Agency (CBSA)
Related Class of Record Number:	CBSA ADM 132
Personal Information Bank:	Traveller Declaration cards PPU 018
Government Official Responsible for PIA:	Vice President, Programs Branch
Delegate for section 10 of the <i>Privacy Act</i> :	ATI and Privacy Director, Dan Proulx

EXECUTIVE SUMMARY

Primary Inspection Kiosk

The CBSA's next generation Primary Inspection Kiosk (PIK) was one of the recommendations put forth by a dedicated Air Traveller Task Force, established in late 2013 with a mandate to develop a strategy to support projected future changes in Canada Border Services Agency's (CBSA) air mode operational environment. Smart border management includes modern services that leverage technology to assist in reducing wait times and congestion at Canada's busiest airports.

Deployment of PIK across Canada's international airports is scheduled to begin in early 2017. PIK will replace the Automated Border Clearance (ABC) kiosks, currently in operation at the international airports of Vancouver, Montreal Pierre-Elliott Trudeau and Toronto Lester B. Pearson. PIK will also expand the population eligible to use a self-service kiosk to include visa-exempt and visa-required foreign nationals.

Upon arrival in Canada, travellers will soon use a next-generation PIK to verify their travel documents, confirm their identity and complete an on-screen declaration. Those looking to save more time can complete their declaration in advance using the CanBorder - eDeclaration mobile application (app) and scan their quick response (QR) code at a kiosk upon arrival.

PIK represents the next evolution in automating Canada's international air ports of entry (POE), in partnership with Airport Authorities (AAs). The kiosk, owned and maintained by AAs, is a tool designed to capture and transmit traveller data securely to CBSA back-end systems, so the CBSA can authenticate an individual's travel documents and identity, and render a recommendation on customs and immigration admissibility. All travellers will continue to see a CBSA officer and some travellers, as occurs today, will be referred for additional questioning or inspection.

Through PIK, the CBSA will improve border security while streamlining service for all travellers entering Canada. By automating administrative tasks, CBSA officers will be freed up to focus on judgement-based and enforcement activities at ports of entry.

The on-screen declaration and mobile app will also allow the CBSA to phase out the current Declaration Card distributed on-board aircraft, reducing paper consumption and saving roughly \$10 million per year through digital service delivery.

Deployment of PIK to the top ten airports is expected to commence March 2017. The airports scheduled for priority deployment of PIK include Ottawa, Toronto, Montreal, Vancouver, Edmonton, Halifax, Winnipeg, Calgary, Billy Bishop and Quebec City airports. Additional airport deployments will be negotiated with interested airport authorities, subject to CBSA capacity.

Protecting Your Personal Information

The following personal information elements related to the traveller will be managed by the PIK¹

Name	Place of residence (Country and Province/State)
Facial photo	Citizenship / Nationality
Duration of absence from Canada (residents only)	Date of birth
Travel document information	Traveller's declaration (e.g., goods, currency, food, etc.)
Duration of stay in Canada (visitors only)	Signature (occurs as attestation on the PIK)
Purpose of Trip (Foreign nationals only)	

While the kiosk and mobile app are new tools, the CBSA's collection of information from travellers arriving by air remains largely unchanged with the exception of the facial photo captured at the kiosk. In fact, by moving to an electronic declaration, the CBSA will be reducing the number of data elements captured to the minimum required for traveller processing, and will increase the integrity of data collection and the security of data transmission.

The collection of information will be facilitated by PIK; no personal information will be stored on the kiosk itself. All information collected will be transferred securely over dedicated lines to CBSA information holdings and purged from the kiosk upon termination of each traveller session.

The mobile app operates without any connection to CBSA systems (i.e., in airplane mode) and retains only basic, non-protected, traveller information, used to pre-populate a portion of the kiosk data entry. Declarations on the app are deleted after 24 hours, and may be manually deleted at any time.

The kiosk and app are tools that will collect information directly from the traveller and verify it against information that is already held within CBSA information holdings. In keeping with the CBSA's current Memorandum of Understanding, information will be disclosed to Statistics Canada (StatCan) for statistical analysis purposes. As per the CBSA's existing practices, in the event it is required for enforcement, program integrity or to address health and safety concerns, information may be requested on a case-by-case basis by law enforcement partners, Employment and Social Development Canada (ESDC) and the Public Health Agency of Canada (PHAC) respectively.

All information collected will be held within the CBSA's existing Integrated Customs System (ICS) platform. ICS is a common platform that encompasses both commercial and passenger-traveller streams and is comprised of a number of components (e.g., Passage History, Secondary Processing, Passenger Information System).

¹ Specific details concerning the collection of these elements are outlined in Section 3.

ABBREVIATIONS AND ACRONYMS

ABC	Automated Border Clearance
ATIP	Access to Information and Privacy
BSO	Border Services Officer
CBSA	Canada Border Services Agency
COR	Class of Record
DSO	Departmental Security Officer
EI	Employment Insurance
EPIL	Electronic Primary Inspection Line
ESDC	Employment and Social Development Canada
FA	Formal Arrangement
GOC	Government of Canada
GSP	Government of Canada Security Policy
HQ	Headquarters
HTTPS	Hypertext Transfer Protocol [Secure]
ID	Identification
IRCC	Immigration, Refugees and Citizenship Canada
ISA	Information Sharing Agreement
IT/IM	Information Technology/Information Management
LAC	Library and Archives Canada
MOU	Memorandum of Understanding
MRZ	Machine Readable Zone
OGD	Other Government Department
OPC	Office of the Privacy Commissioner of Canada
PA	<i>Privacy Act</i>
PHAC	Public Health Agency of Canada
PAXIS	Passenger Information System
PI	Personal Information
PIA	Privacy Impact Assessment
PIB	Personal Information Bank
PKD	Public Key Directory
PNS	Privacy Notice Statement
PoE	Port of Entry

SAR	Security Assessment Report
SOAP	Simple Object Access Protocol
SOS	Statement of Sensitivity
SPPH	Secondary Processing and Passage History
StatCan	Statistics Canada
TBS	Treasury Board Secretariat
TLS	Transport Layer Security
TRA	Threat and Risk Assessment
VP	Vice-President
VPN	Virtual Private Network

DEFINITIONS

Action Plan	The Action Plan describes the steps that the Program will take to address risks that have been identified by ATI and Privacy Division, Office of the Privacy Commissioner of Canada (OPC) and Treasury Board Secretariat (TBS).
Administrative purpose	The <i>Privacy Act</i> defines an “administrative purpose” to be the use of an individual’s personal information in a decision-making process that directly affects that individual.
Consistent use	Is a use that has a reasonable and direct connection to the original purpose(s) for which the information was obtained or compiled. This means that the original purpose and the proposed purpose are so closely related that the individual would expect that the information would be used for the consistent purpose, even if the use is not spelled out.
Data Matching	A comparison of personal data obtained from a variety of sources, including personal information banks, for the purpose of making decisions about the individuals to whom the data pertains. Data matching is a specialized activity involving the collection, use and disclosure of personal information that is subject to the various requirements of the <i>Privacy Act</i> .
Info Source	Is a series of annual TBS publications in which government institutions are required to describe their institutions, program responsibilities and information holdings, including PIBs and classes of personal information. The descriptions are to contain sufficient clarity and detail to facilitate the exercise of the right of access under the <i>Privacy Act</i> . Data-matching activities, use of the SIN and all activities for which privacy impact assessments were conducted have to be cited in <i>Info Source</i> PIBs, as applicable. The <i>Info Source</i> publications also provide contact information for government institutions as well as summaries of court cases and statistics on access requests.
Personal Information	Information about an identifiable individual as defined in section 3 of the <i>Privacy Act</i> . This definition, although lengthy, is not exhaustive, as indicated by the introductory phrase, “including, without restricting the generality of the foregoing”. Information that is not specifically mentioned in the list may still be included in the definition of personal information if it qualifies as “information about an identifiable individual”.
Personal Information Bank	Is a description of personal information that is organized and retrievable by a person's name or by an identifying number, symbol or other particular assigned only to that person. The personal information described in the personal information bank has been used, is being used, or is available for an administrative purpose and is under the control of a government institution.
Privacy	The OPC describes “privacy” as “... the right to control access to one's person and information about one's self. The right to privacy means that individuals get to decide what and how much information to give up, to whom it is given, and for what uses.”

SECTION 1 - OVERVIEW AND INITIATION

Report Objectives

This report is a Privacy Impact Assessment (PIA) for the Primary Inspection Kiosk (PIK) initiative, including the CanBorder-eDeclaration mobile application. PIK is the evolution of the Automated Border Clearance (ABC) initiative, for the Canada Border Services Agency (CBSA). The PIK initiative will introduce increased functionality in support of both facilitation and security, including complete on-screen traveller declaration and the elimination of the paper E311 declaration card, and will begin to use the International Civil Aviation Organization (ICAO) standards to authenticate a traveller's documents and identity. In addition, the PIK initiative will expand the population eligible to use the PIK, including visa-exempt and visa-required foreign nationals.

The objectives of this PIA are:

- to review the business processes in order to identify the data flow of personal information;
- to analyze the collection, use, disclosure and retention of personal information;
- to determine if there are privacy risks associated with the expansion of the PIK; and
- to provide recommendations on the mitigation or elimination of the risks.

An initial PIA and one addendum related to ABC have been provided to the Office of the Privacy Commissioner (OPC) and initial meetings discussed the evolution of primary inspections at Canadian airports. The information presented in this report follows the Treasury Board of Canada Secretariat (TBS) PIA policy and guidelines.

The purpose of a PIA process is to ensure that privacy is considered throughout the project development cycle. The results of a PIA are a documented guarantee that privacy issues have been identified and adequately addressed.

Government Institution: CBSA / Programs Branch

Government Official Responsible for the Privacy Impact Assessment	Head of the government institution / Delegate for section 10 of the <i>Privacy Act</i>
Martin Bolduc, Vice President, Programs Branch	Dan Proulx, Director, Access to Information and Privacy Division

Name of Program or Activity of the Government Institution:

This initiative relates to the 1.3 Admissibility Determination sub-activity and the 1.3.2 Air Mode sub-sub-activity.

Description of Program or Activity:

1.3 Admissibility Determination – through the Admissibility Determination program, the CBSA develops, maintains and administers the policies, regulations, procedures and partnerships that enable border services officers to intercept people and goods that are inadmissible to Canada, and to process admissible people and goods within established service standards. In addition, the Agency develops, maintains and administers the policies, regulations, procedures and partnerships to control the export of goods from Canada. In the traveller stream, border services officers question people upon arrival to determine if they and their personal goods meet the requirements of applicable legislation and regulations to enter Canada. Border services officers (BSOs) will then make a decision to grant entry or refer a person for further processing (e.g., payment of duties and taxes, issuance of a document), and/or for a physical examination.

1.3.2 Air Mode – The Air Program identifies and intercepts people and goods that are inadmissible to Canada seeking entry at designated airports while ensuring that admissible people and goods are processed within established service standards. Upon arrival, border services officers conduct interviews of persons seeking entry into Canada, aided by electronic pre-arrival risk-assessment information submitted by the airlines. CBSA officers make a decision to admit the person or refer them for further processing (e.g., payment of duties and taxes, issuance of a document) or examination. For private and corporate aircraft and general aviation traffic reporting through the Telephone Reporting Centre, various checks are conducted by means of the telephone reporting system. BSOs make a decision to admit people or refer them for further processing or examination. To assist border services officers in their examinations, detection tools such as detector dogs and ion scanners may be used. People and goods found to be in violation of the applicable legislation and/or regulations may be subject to a monetary penalty, seizure or denied entry to Canada.

Description of the class of records associated with the program or activity:

Interdepartmental and Intergovernmental Relations Program

Description: Describes records relating to the Interdepartmental and Intergovernmental Relations Program which describes written information sharing collaborative agreements between the CBSA and federal departments. Records may also include Travellers Declaration cards, Casual Goods Accounting Documents, records or reports from electronic systems used to administer or manage the program including the Travellers Entry Processing System (TEPS), the Customs Commercial System (CCS), the Facility for Information Retrieval Management (FIRM) and the Travellers National Database System (TRANDS).

Document Types: Memoranda of Understanding, Letters of Understanding, Information Sharing Agreements, policy, guidance materials, Memos and Forms.

Record Number: CBSA ADM 132

Class of Record Number:

CBSA ADM 132

- ☐ Proposal for a New Personal Information Bank
- ☒ Proposal to modify an existing Personal Information Bank - identify PIB registration number and current description:

Traveller Declaration

Description: This bank describes information used in support of the Canada Border Services Agency (CBSA) Travellers Border Programs, specifically the E311 Traveller Declaration card (E311) and digital declaration at the Primary Inspection Kiosk. The personal information may include name, date of birth, citizenship, visual image of traveller, travel document information, place of residence (Province/State and Country) and signature. For visitors to Canada, the duration of stay in Canada and if the duty-free allowances are exceeded; for residents of Canada, the date of departure or duration of absence from Canada and the value of goods – CAN\$ purchased or received abroad (including gifts, alcohol and tobacco). In addition, responses to a number of questions are also requested: the origin of the flight, purpose of trip, goods brought or unaccompanied in Canada, currency and/or monetary instruments totalling CAN\$ 10,000 or more, and if a visit has been made or scheduled to a farm.

Class of Individuals: All persons entering Canada, including but not limited to, Canadian citizens, permanent residents, visitors, crew members, diplomats, military personnel, refugees, immigrants, former residents.

Purpose: The personal information is collected pursuant to the *Customs Act*, *Customs Tariff*, *Immigration and Refugee and Protection Act (IRPA)*, *Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA)* and Subsection 5(3) of the Reporting of Imported Goods Regulations for the purposes of facilitating compliance with travellers' obligations to report their goods in writing upon entry into Canada including the collection of duty and taxes owing on those goods imported into Canada and to administer laws that enforce, prohibit, control and regulate the importation of goods into Canada and the movement of people coming into Canada.

Consistent Uses: Information may be disclosed internally to the CBSA Enforcement and Intelligence Operations Directorate for the purposes of assisting CBSA's enforcement program, and criminal investigations operations. Information may be disclosed externally to Employment and Social Development Canada (ESDC) and the Public Health Agency of Canada for the purposes of Program integrity; refer to: Employment Benefits, Support Measures and Other Programs ESDC PPU 293 and Traveler Illness Reports PHAC PPU 071. Information may also be disclosed to Statistics Canada for the purposes of evaluation and statistical reporting. Information may also be disclosed to police forces, investigative agencies and other countries for the purposes of criminal investigations law enforcement.

Retention and Disposal Standards: Files are retained for seven years from the date stamped on the traveller's declaration card (or date stamped on the traveller receipt when the traveller uses the Automated Border Clearance, the Primary Inspection Kiosk or NEXUS kiosk). After this period, the records are destroyed.

RDA Number: 2000/033

Related Record Number: CBSA ADM 132

TBS Registration: 002271

Bank Number: CBSA PPU 018

Legal Authority for Program or Activity:

Legal authority for the collection of personal information through the automated primary inspection process facilitated through PIK, is derived from multiple, inter-related legislations and regulations.

- Information required for the regulation of goods (import/export) is derived from one legislation and supporting regulations. 1) Section 12 of the *Customs Act*, which states, "all goods that are imported shall, except in such circumstances and subject to such conditions as may be prescribed, be reported at the nearest customs office designated for that purpose that is open for business." And 2) Section 5(3) of the *Reporting of Imported Goods Regulations*, which states, "Goods that are imported by a person arriving in Canada on board a commercial passenger conveyance other than a bus shall be reported in writing."
- Information required from individuals as they request entry into Canada is derived from two legislations. 1) Section 11 of the *Customs Act*, which states, "every person arriving in Canada shall, except in such circumstances and subject to such conditions as may be prescribed, enter Canada only at a customs office designated for that purpose that is open for business and without delay present himself or herself to an officer and answer truthfully any questions asked by the officer in the performance of his or her duties under this or any other Act of Parliament." And 2) Section 18(1) of the *Immigration and Refugee Protection Act* which states, "Every person seeking to enter Canada must appear for an examination to determine whether that person has a right to enter Canada or is or may become authorized to enter and remain in Canada."

In addition to these specific legal authorities, information is also collected under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, as well as associated regulations made thereunder such as the *Cross-border Currency and Monetary Instruments Reporting Regulations*. Subsection 12(1) of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* states, "every person or entity referred to in subsection (3) shall report to an officer, in accordance with the regulations, the importation or exportation of currency or monetary instruments of a value equal to or greater than the prescribed amount."

Program legislation as defined in the *Customs Act* "means any other Act of Parliament or any instrument made under it, or any part of such an Act or instrument,

(a) that the Governor in Council or Parliament authorizes the Minister, the Agency, the President or an employee of the Agency to administer and enforce, including the *Customs Act*, the *Customs Tariff*, the *Excise Act*, the *Excise Act, 2001*, the *Immigration and Refugee Protection Act* and the *Special Import Measures Act*;

(b) that the Governor in Council or Parliament authorizes the Minister, the Agency, the President or an employee of the Agency to enforce, including the *Agriculture and Agri-Food Administrative Monetary Penalties Act*, the *Canada Agricultural Products Act*, the *Feeds Act*, the *Fertilizers Act*, the *Fish Inspection Act*, the *Health of Animals Act*, the *Meat Inspection Act*, the *Plant Protection Act* and the *Seeds Act*;

(c) under which the Minister or another minister authorizes the Agency, the President or an employee of the Agency to administer a program or carry out an activity; or

(d) under which duties or taxes collected and paid pursuant to the *Customs Act* are imposed."

Summary of the initiative:

The CBSA, like an increasing number of countries worldwide, is expanding its automated border solution to improve the Agency's capacity to deal with sharp spikes in traveller volumes within limited airport space, reduce border wait times, improve traveller identity and risk assessments, and reduce the use of paper to perform administrative functions.

PIK is the next generation of kiosks that will replace the current ABC kiosks in place at the international airports of Vancouver, Montreal Pierre-Elliott Trudeau and Toronto Lester B. Pearson. A final deployment of ABC was in Calgary International Airport in October 2016. A PIA has previously been submitted to the Office of the Privacy Commissioner for the ABC initiative.

Upon arrival in Canada, travellers will soon use a next-generation PIK to verify their travel documents, confirm their identity and complete an on-screen declaration. Those looking to save more time can complete their declaration in advance using the CanBorder - eDeclaration mobile application (app) and scan their quick response (QR) code at a kiosk upon arrival.

In summary, PIK 1.0 will support the automation of existing manual processes, extend eligibility to all foreign nationals (FNs), introduce ePassport Public Key Directory (PKD) validation, biometric passport verification through facial authentication, and move to replace E311 form by introducing the capture of on-screen traveller declarations.

Deployment of PIK to the top ten airports is expected to commence in March 2017. The airports scheduled for priority deployment of PIK include Ottawa, Toronto, Montreal, Vancouver, Edmonton, Halifax, Winnipeg, Calgary, Billy Bishop and Quebec City airports.

Eligible Travellers

For PIK, eligible travellers include Canadian citizens, Canadian Permanent Residents, U.S. citizens and all other Foreign Nationals, both visa-exempt and visa-required.

Although the CBSA is targeting to direct 100% of travellers for processing via PIK, a subset of travellers will choose or be directed to in-person processing for a number of reasons including language, technology aversion, documentation issues, or age. Each CBSA Hall employing PIK will retain a number of traditional PIL booths for in-person processing.

In a number of scenarios the client will ultimately be referred to in-person processing by a CBSA officer. The following non-exhaustive list provides examples of travellers who would be eligible to use PIK; however PIK will invoke exception processing in order to ultimately refer them to in-person* processing:

- Eligible Foreign National travellers with an expired travel document
- Travellers without a machine-readable travel document
- Unaccompanied minor(s) (i.e., under 16 years of age)

* A PIA has not been conducted for traditional Primary inspection by a BSO. As a result, privacy risks of in-person processing for travellers opting not to use PIK are unknown.

Kiosk Processing

To use the kiosk, the traveller activates the kiosk touch screen and follows the on-screen instructions to complete their primary processing session. The traveller will be directed to insert their travel document into the PIK travel document reader, which will scan the Machine Readable Zone (MRZ) and initiate a passage risk assessment against CBSA systems.

Travel Document Validation

For travellers who present a “non-ePassport” PIK will process the traveller fully and record an indicator on the receipt, to prompt the Podium Officer to conduct a document and identity check on the traveller. For travellers who present an “ePassport” PIK will conduct an ePassport validation to confirm authenticity of the document and traveller, using the International Civil Aviation Organization (ICAO) Public Key Directory (PKD). This process will confirm that an ePassport has been issued by the jurisdiction with the delegated authority, that biographic and biometric information has not been altered, provide authentication to ensure the document is not a clone, and verify that the document does not appear under ICAO’s Certificate Revocation List (CRL).

Facial Authentication

PIK will provide all travellers with on-screen directions to present for a photo (facial image capture). The traveller’s photo will be printed on the traveller’s PIK receipt to be used by BSOs throughout the CBSA Hall in order to confirm traveller identity and link each traveller with the receipt, and for non-ePassports with the travel document as well.

For ePassports, facial authentication processing will also take place. The PIK will open the chip on the ePassport, access the traveller’s digital image stored on the chip, and compare it to the photo taken of the traveller. The comparison of the two images to achieve a match will verify the traveller’s identity based on an established match threshold as well as link the traveller to the ePassport presented. If the check shows a “below threshold” match, a CBSA officer will manually conduct a review of the traveller against the photo in their passport and make a determination as to whether they need to be referred for additional questioning. The manual review by a CBSA officer of the traveller against the photo in their passport will also take place for non-ePassport holders. The volume of the latter is expected to be low as more than 110 countries are issuing ePassports.

The photo captured at the kiosk will not be stored separately in the CBSA systems; however, as it is printed on the kiosk receipt, it will be embedded in the PIK receipt image stored in the CBSA passage history database.

On-Screen Traveller Declaration

After PIK takes the traveller’s photo, the on-screen traveller declaration process begins. The traveller is directed through a series of required customs and immigration questions. The on-screen declaration eliminates the need to complete the paper E311 Declaration Card, currently distributed on airplanes arriving in Canada.

System Queries

PIK will query existing CBSA systems such as Interdiction and Border Alert System (IBAS) to retrieve Immigration documents, verify citizenship/immigration status, immigration lookouts (EII), and verify the travel document against the Lost, stolen, Fraudulent Document (LSFD) database and TUSCAN, query Integrated Custom Enforcement System (ICES) to retrieve any existing CBSA customs and law enforcement lookouts, and query Passenger Information System (PAXIS) to retrieve passenger flight number and identify flight crew.

The system-generated results of the kiosk passage event, ePassport validation, facial match processing, and responses to declaration questions, will use a set of pre-derived business rules (e.g., whether the photo match meets the established threshold, whether the declared goods/currency is within the allowed exemption limit) to determine if a traveller is released to collect their bags, or referred for additional questioning.

PIK Receipt

When all system queries have been completed and the traveller's on-screen declaration has been finalized and submitted, PIK will print a receipt for the traveller(s) for use by CBSA personnel throughout the CBSA Hall.

All PIK receipts will include the traveller's photo captured by the kiosk, certain biographical data of the traveller, travel document number, the traveller's flight details (i.e., air carrier code and flight number) in addition to CBSA refer-release coding. All PIK receipts will be collected by CBSA officers before travellers exit the secure area. In general, paper receipts will be destroyed, however, should a traveller be referred for additional questioning and an officer mark their receipt, the paper copy of the receipt would be added to their file as required. The CBSA will retain an electronic image of the receipt in accordance with access to information and privacy requirements.

CanBorder – eDeclaration Mobile Application

PIK will also provide an expedited functionality for travellers to expedite their on-screen declaration by using the CanBorder-eDeclaration app. The app will be available for download for free on portable electronic devices (e.g., smartphone, tablet) through third party distributors such as Apple, Google, and BlackBerry World.

App users will be prompted, at the beginning of the kiosk session, to scan their eDeclaration QR code which will pre-populate the kiosk screens, reduce typing and expedite processing at the kiosk. Clarifying questions will be presented on-screen as required, and the traveller will be presented with an editable declaration summary.

Clients who download the mobile app will follow the instructions to create traveller profiles for everyone in their travel group. Up to five traveller profiles can be stored within the app. The app is designed to limit data collection and ensure privacy. No biographic or travel document information is stored in the app. Each traveller profile consists of a nickname, and place of residence, as defined by Country (and Province/State for Canadian and U.S. residents). Travellers complete their electronic declaration by using the "My Declaration" function within the app. Data elements collected include:

- Flight Information (Arrival airport and arriving from)
- Travel Group (confirmation of all travellers declaring together)

- Duration of Absence from Canada or Duration of Stay in Canada
- Personal Exemptions / Visitor Allowances
- Value of goods (for residents exceeding their personal exemption limits only)
- OGD Questions (firearms, commercial goods, agricultural products, currency, unaccompanied goods, and farm visit)

Each My Declaration concludes with an editable review screen. Travellers must also review a Privacy Notice Statement before their declaration can be finalized on the app. Upon completion, the client is issued a QR code. A review of the Privacy Notice Statement is required each time My Declaration is completed.

Upon arrival in Canada, the client scans their QR code at a Primary Inspection Kiosk. Each traveller is prompted, by travel profile nickname, to scan their travel document and present for a picture, at which time each traveller's declaration is reconciled against their legal name. The data transmitted to the kiosk by scanning the QR code, pre-populated their declaration and is presented as an editable summary for them to confirm.

The traveller must certify their declaration at the end of the PIK session, and the session results are printed on a paper receipt generated by the kiosk.

The mobile app has been designed to ensure the protection of privacy and personal information. Once downloaded on a client's mobile device (e.g. tablet or smartphone), the app operates entirely in airplane mode. The stand-alone application does not require data use/Wi-Fi access, does not connect to CBSA systems; no information is transmitted to the CBSA until the QR code is scanned at the kiosk. Each QR code expires 24 hours after it is issued; at which time all declaration data is deleted from the app. Clients can also delete their QR code or manually clear their declaration data at any time.

Interaction with CBSA Officers

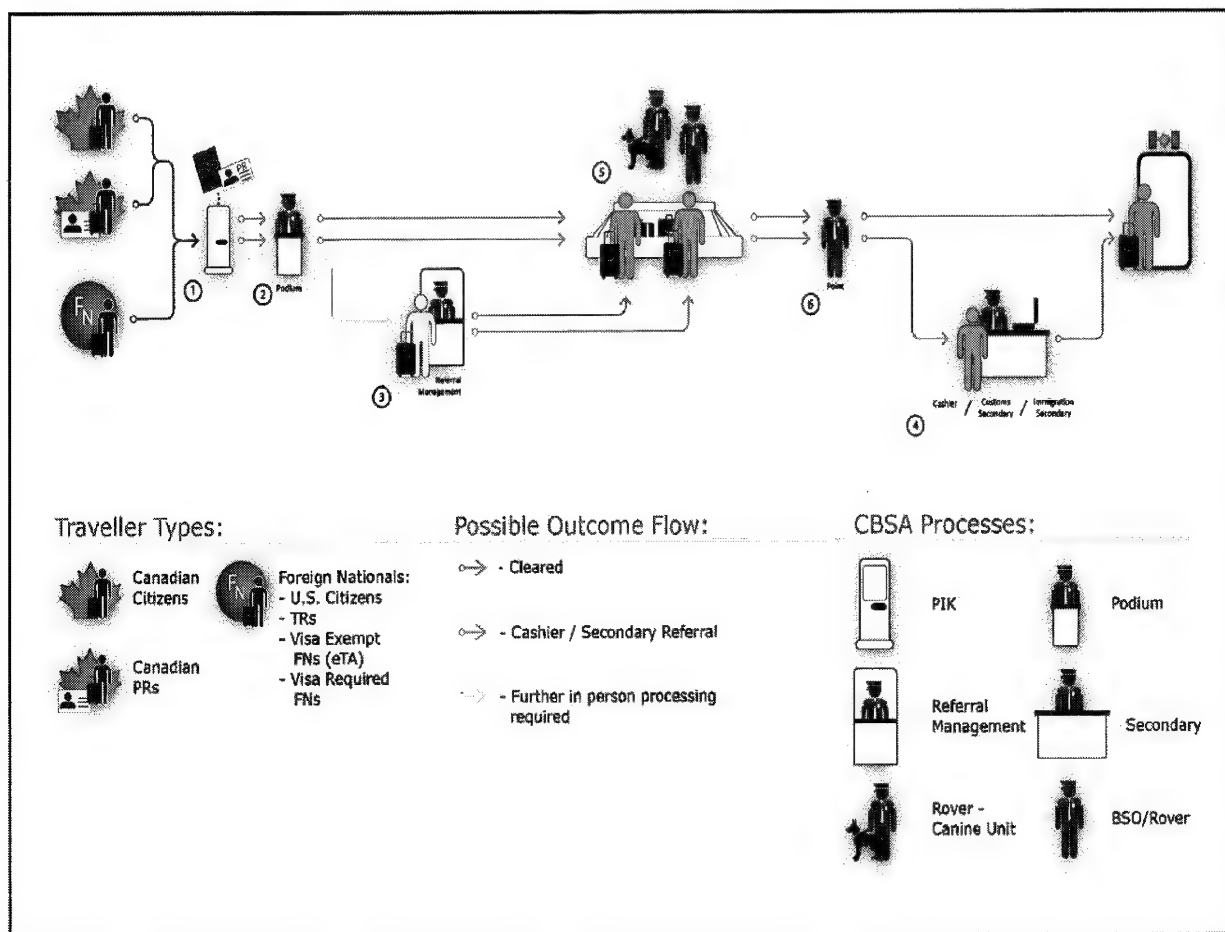
All travellers will continue to see a CBSA officer as part of routine processing. CBSA officers in the role of Podium Officer, Referral Officer, Roving Officer, or Egress Officer, will have the discretion to override the PIK release recommendation, and can ask travellers additional questions and refer them to Immigration and/or Customs Secondary for further examination and determination of admissibility.

Once processed by PIK, travellers will fall within the following "status" categories:

Status	Description
>> Green	Recommended for release by PIK. The traveller proceeds to the Podium Officer who directs the traveller to the baggage hall/Egress. The Podium Officer (and in fact any Officer in the CBSA hall) retains the right to overturn the green status and refer the traveller to the Referral Officer and/or Secondary if deemed necessary.
>> Red	Referred by PIK to Customs or Immigration Secondary. The traveller proceeds to the Podium Officer who further directs the traveller to the baggage hall/Egress, or in some instances, directly to the secondary processing location.

Yellow	Identified by PIK and/or the Podium Officer for further in-person processing/questioning. The Podium Officer directs the traveller to the Referral Officer. Following a brief interview by the Referral Officer, the traveller is released, the referral is maintained, or a new referral is created and the traveller is directed to the baggage hall/Egress, or in some instances, directly to Secondary processing location.
---------------	---

The following diagram displays the PIK operational design and process flow:



SECTION 2 - RISK AREA IDENTIFICATION AND CATEGORIZATION

For Section 2, check the appropriate box that describes the level of risk related to your program or activity and provide details as indicated. Please note that answering "yes" or "no" without providing explanatory details may trigger more questions from the Office of the Privacy Commissioner.

Please ensure that the details provided respond to these 4 elements:

1. **Necessary:** It must be demonstrably necessary in order to meet some specific need
2. **Effective:** It must be demonstrably likely to be effective in achieving its intended purpose. In other words, it must be likely to actually make us significantly safer, not just make us feel safer.
3. **Proportionate:** The intrusion on privacy must be proportional to the security benefit to be derived.
4. **Minimal:** and it must be demonstrable that no other, less privacy-intrusive, measure would suffice to achieve the same purpose

Type of Program or Activity	Level of Risk
Program or activity that does NOT involve a decision about an identifiable individual	<input type="checkbox"/> 1
Administration of Programs / Activity and Services	<input type="checkbox"/> 2
Compliance / Regulatory investigations and enforcement	<input checked="" type="checkbox"/> 3
Criminal investigation and enforcement / National Security	<input checked="" type="checkbox"/> 4

Details: PIK collects the required personal information directly from the traveller for the determination of admissibility and the identification of any previous enforcement actions/ lookouts or affirmative answers to the declaration questions that would result in a referral to Secondary (i.e., Customs, Immigration, OGD or cash). Any information collected on the mobile application is transferred to the kiosk by scanning the QR code upon arrival; queries of CBSA systems remains at the kiosk.

The information collected from travellers through PIK is the same as the information collected at Primary Inspection Line with the exception of capturing the photo at the kiosk and printing on the receipt. In fact, with PIK, the CBSA will be reducing the data elements collected to the minimum required for traveller processing. For example, instead of full address, travellers will be asked for only province for Canadian citizens and country for foreign nationals, purpose of trip will only be collected from foreign nationals.

Necessity

The standard border wait time at an airport is set at 20 minutes or less and is used as a measure of efficiency. A CBSA study (draft) finds that a wait-time higher than 20 minutes at the top eight Canadian airports have cost billions of dollars to Canadian economy. The estimates suggest that in FY 2016-16, 2.1 million international travellers decided not to travel to Canada due to higher border wait time.

The photo printed on the kiosk receipt increases the confidence with which BSOs throughout the border

clearance continuum verify and confirm a traveller's identity. The photo is essential in order to reconcile the traveller presenting themselves to a BSO with the self-service kiosk risk assessment results printed on the receipt. In essence, the photo on the PIK receipt allows for the highest level of confidence in traveller identification under a self-service kiosk operational model, and does so without a negative impact on border wait times.

Currently, under the ABC model, the Document Verification Officer (DVO) whom travellers see post-kiosk transaction has to open each passport, look for the traveller name and compare that to the name printed on the kiosk receipt. For program integrity purposes, the officer has to pay careful attention especially where names are complex (long, hyphenated, etc.) and make sure it matches the name printed on the receipt. This process slows down the movement of travellers at DVO. With increasing traveller volumes at Canada's top ten airports and limited infrastructure and space within the CBSA Hall, the slowdown of travellers' throughput at DVO has ripple effect causing not only border wait times, but bottlenecks, congestion in CBSA Hall and beyond extending to corridors, and flight delays or missed flights. With travellers increasingly accustomed to automation and fast processing the bottlenecks and long wait time leads to frustration, complaints and criticism as was recently reported by several media outlets.

When presented with a receipt containing the traveller's photo, the BSO at Podium (same as DVO under ABC) can quickly compare the photo on the receipt with the traveller before him/her, thereby streamlining the process and traveller flow at Podium. For ePassport cases where the system returns a below threshold photo match score, the kiosk will print a notification to Podium. The BSO at Podium would be able to verify if the low match confidence score is due to a bad photo captured at the kiosk (e.g., the individual's face is not visible because they were looking to the side or down) and resolve the issue quickly with minimal delay to the traveller. In the absence of a photo on the receipt, all such cases will have to be referred for further investigation to ensure the travel document is genuine and the chip has not been tampered with.

Effectiveness

Proportionality

In *R. v. Simmons* (1988), the Supreme Court of Canada recognized that there is a lowered expectation of privacy in the border context given the importance that effective border management has on the well-being of the nation.² Further, the Ontario Court of Appeal reaffirmed the importance of effective border management in the *R. v. Jones* (2006) decision by recognizing Canada's control over its border "as a societal interest of sufficient importance to be characterized as a principle of fundamental justice" given that effective border management serves a number of crucial social interests that benefit the Canadian public.³

The adoption of self-service kiosk for air traveller processing is derived from the Government of Canada's need to process rising volumes of international air traveller within the standard wait time while safeguarding border integrity and national security. The PIK receipt forms an integral part of the kiosk processing and the photo on the receipt is essential in order to link a traveller and the results of risk assessment processing that occur during the self-service passage event. Removing the photo from the PIK receipt would be the equivalent of removing the photo from a piece of identification.

Public Safety and National Security – Ability to effectively intercept high-risk travellers seeking entry to Canada or the goods they carry (e.g., terrorists, members of transnational and organized crime, child sex offenders, illicit, prohibited or controlled goods, etc.) by linking the traveller with their receipt through the photo printed on the receipt.

Program Integrity – Better protect the integrity of Canada's immigration program by preventing and identifying

² *R. v. Simmons* 1988 SCC 495 at para 49.

³ *R. v. Jones*. 2006 OCA para 31

cases of non-compliance, fraud and misrepresentation.

Minimal Intrusiveness

The CBSA has examined less privacy-intrusive measures, including status quo and technological solution.

Status quo – as demonstrated above, status quo (i.e., opening the passport of each traveller to compare the name of the holder or travel document number with the name or travel document number printed on the kiosk receipt) is operationally inefficient and simply not feasible as it will cause congestion in the CBSA Hall, flight delay/missed flights, and failure to meet the CBSA standard border wait time. Travellers have been voicing their frustration at the long border wait times at airports and are requesting the Government to revisit its processes to make the wait time shorter.

Some high-risk travellers may not be identified and intercepted, resulting in individuals presenting a potential risk to national security and public safety and controlled, regulated, or prohibited goods, allowed entry to Canada.

Technological Solutions – the CBSA looked into the option of a handheld device for Podium and Egress. Under this option, a barcode will be printed on the kiosk receipt for BSOs to scan through the handheld device to confirm identity, link traveller to the receipt and confirm refer / release status. Such device would help the BSOs at Egress make a quick and accurate decision on whether the traveller should be referred to Secondary for further examination or be allowed to proceed to exit, However, due to the time, effort and cost required to develop this tool, it was determined that this option is not feasible at this time especially in light of current fiscal restraint. That said, the handheld device is being put forward for the next PIK iteration, PIK 2.0.

Travellers are notified in the Privacy Notice Statement that their photo will be captured at the kiosk and are allowed the option to opt out of using the kiosk and using in-person process instead.

Type of Personal Information Involved and Context

Level of Risk

Only personal information, with no contextual sensitivities, collected directly from the individual or provided with the consent of the individual for disclosure under an authorized program.

☐ 1

Personal information, with no contextual sensitivities after the time of collection, provided by the individual with consent to also use personal information held by another source.

☐ 2

Social Insurance Number, medical, financial or other sensitive personal information and/or the context surrounding the personal information is sensitive. Personal information of minors or incompetent individuals or involving a representative acting on behalf of the individual.

☒ 3

Sensitive personal information, including detailed profiles, allegations or suspicions, bodily samples and/or the context surrounding the personal information is particularly sensitive.

☐ 4

Details: Information is provided directly by the traveller, by scanning their travel document, presenting for a photo and answering the declaration questions. On its own, the information has little contextual sensitivity.

This information is compared against information found in other CBSA information sources to determine whether or not the travellers are to be referred to Secondary for a more comprehensive investigation. This information may have originated by direct or indirect means. Specific data elements of the personal information will be limited to Biographic Entry Data, specifically: Name (First/Given Name, Last Name/Surname), Date of Birth, Province for residents, and Country for Foreign nationals, Nationality/Citizenship, Gender, Document Type, Document Number, Document Country of Issuance, Duration of Absence from Canada, Arriving Flight Number, and Purpose of Travel (except for residents of Canada). The risk level 3 is identified as information about minors must be collected indirectly. The SIN, medical, and financial information are not collected.

PIK process and information flow is demonstrated in Diagram 1 in Section 4.1. Data elements exchanged between the Kiosk and CBSA backend systems during traveller session, context, data elements stored by the CBSA and the CBSA systems in which the data is stored are all listed in the table in Section 4.1. The flow of information from traveller to the kiosk to CBSA and back to the kiosk are depicted in diagrams 2, 3 and 4 in Section 4.1. Note: the information in the table correspond to the steps/information flow presented in the diagram 2,3 and 4.

Primary Inspection Kiosk	PIA
--------------------------	-----

Program or Activity Partners and Private Sector Involvement	Level of Risk
Within the CBSA (amongst one or more programs within the CBSA)	<input checked="" type="checkbox"/> 1
With other federal institutions	<input checked="" type="checkbox"/> 2
With other or a combination of federal/ provincial and/or municipal government(s)	<input type="checkbox"/> 3
Private sector organizations or international organizations or foreign governments	<input type="checkbox"/> 4

Details: Primary inspection processing is completed by CBSA officials. While this occurs on site at Canadian airports, the Airport Authority does not have access to the information collected and is not part of program delivery. A Service Level Agreement (SLA), signed with each Airport Authority prior to PIK implementation governs the relationship and outlines each party's obligations with respect to the kiosk device. The CBSA, as a full partner in kiosk design, testing and activation is responsible to ensure the proper functioning of the kiosk and adherence to information management and information security requirements. Information collected is encrypted at the kiosk before being securely transferred through a VPN to CBSA back-end systems, where queries are conducted and determinations are made. Information is again encrypted before it is sent back to the kiosk. The data is erased from the kiosk in a way to make it irretrievable on completion of the traveller's passage event. At no time will the Airport Authority have access to the information contained in the CBSA back-end systems. Disclosures of information to other government departments occur after processing. In this PIA only disclosure of information to StatCan is addressed, disclosure of information collected through PIK to other government departments (i.e., ESDC) is not addressed as discussions are still in preliminary stages. An amendment to the PIA will be made once an agreement has been reached.

In terms of disclosure of travellers' data to StatCan, currently all paper E311 customs declaration forms are sent to StatCan monthly for scanning to JPEG files (in other words, a "snapshot" is taken of each declaration), and StatCan returns a hard drive to CBSA with the captured E311 JPEG files. Annually, this represents over 20M records that are returned to the CBSA. Other Government Departments leverage this E311 JPEG data as well. With PIK, travellers' data will be captured in discrete data fields, and transferred electronically to and automatically stored in a CBSA repository. The CBSA is developing an automated method to extract selected traveller data and electronically transmit it to StatCan by secure means. The traveller data sharing with StatCan is addressed in more detail in section 4.4.

Duration of the Program or Activity	Level of risk
One time program or activity Typically involves offering a one-time support measure in the form of a grant payment as a social support mechanism.	<input type="checkbox"/> 1
Short-term program A program or activity that supports a short-term goal with an established "sunset" date.	<input type="checkbox"/> 2
Long-term program Existing program that has been modified or is established with no clear "sunset".	<input checked="" type="checkbox"/> 3

Details: The automation of primary processing was one of the recommendations of the Air Traveller Task Force and is a long term initiative for the CBSA. Through the implementation of PIK, infrastructure changes will be made within the CBSA service areas; traditional primary inspection booths will be removed to free up space and improve traveller flow. The CBSA is continuing its deployment of kiosk processing by leveraging technology to

complete additional administrative tasks and broadening the number of travellers eligible for self-service processing.

Implementation of the PIK initiative will automate administrative tasks, freeing up CBSA officers to focus on judgement-based and enforcement activities at ports of entry. All travellers will continue to see a CBSA officer as part of their entry to Canada. The on-screen declaration and mobile app will also allow the CBSA to phase out the current Declaration Card distributed on-board aircraft, reducing paper consumption and saving roughly \$10 million per year through digital service delivery.

Program Population

Level of Risk

- | | |
|---|---------------------------------------|
| The program affects certain employees for internal administrative purposes. | <input type="checkbox"/> 1 |
| The program affects all employees for internal administrative purposes. | <input type="checkbox"/> 2 |
| The program affects certain individuals for external administrative purposes. | <input checked="" type="checkbox"/> 3 |
| The program affects all individuals for external administrative purposes. | <input type="checkbox"/> 4 |

Details: This initiative affects individuals who present themselves at kiosks, seeking entry to Canada at specific airports. Primary processing occurs when an individual seeks entry to Canada, regardless of whether the individual chooses to use a PIK or present themselves to a traditional Primary Inspection Line. While PIK is a new tool, the collection of personal information to support the primary processing, with the exception of collection of the photo, remains largely unchanged.

Technology and Privacy

- | | |
|--|--|
| 6.1 Does the new or modified program or activity involve the implementation of a new electronic system, software or application program including collaborative software (or groupware) that is implemented to support the program or activity in terms of the creation, collection or handling of personal information? | <input checked="" type="checkbox"/> YES
<input type="checkbox"/> NO |
| 6.2 Does the new or modified program or activity require any modifications to IT legacy systems and / or services? | <input checked="" type="checkbox"/> YES
<input type="checkbox"/> NO |
| 6.3 Does the new or modified program or activity involve the implementation of one or more of the following technologies: | |
| 6.3.1 Enhanced identification methods:
This includes biometric technology (i.e. facial recognition, gait analysis, iris scan, fingerprint analysis, voice print, radio frequency identification (RFID), etc...) as well as easy pass technology, new identification cards including magnetic stripe cards, "smart cards" (i.e. identification cards that are embedded with either an antenna or a contact pad that is connected to a microprocessor and a memory chip or only a memory chip with non-programmable logic). | <input checked="" type="checkbox"/> YES
<input type="checkbox"/> NO |

6.3.2 Use of Surveillance:

This includes surveillance technologies such as audio/video recording devices, thermal imaging, recognition devices, RFID, surreptitious surveillance / interception, computer aided monitoring including audit trails, satellite surveillance etc.

☐ YES
☒ NO

6.3.3 Use of automated personal information analysis, personal information matching and knowledge discovery techniques:

For the purposes of the Directive on PIA, CBSA is to identify those activities that involve the use of automated technology to analyze, create, compare, cull, identify or extract personal information elements. Such activities would include personal information matching, record linkage, personal information mining, personal information comparison, knowledge discovery, information filtering or analysis. Such activities involve some form of artificial intelligence and/or machine learning to uncover knowledge (intelligence), trends/patterns or to predict behaviour.

☒ YES
☐ NO

Details: PIK is new solution that provides travellers the ability to enter their personal information and customs declaration directly into a self-service kiosk to transmit to the CBSA. The CBSA will introduce a combination of new services and update existing IT legacy systems and services to support PIK. In terms of new services, the PIK Service handles the orchestration and coordination of primary processing for each traveller. New supporting services include the PIK Management Service, PAXIS Flight Data Service, Travel Document Verification Service, and Passage Notification Service for sharing declaration data with StatCan. Legacy IT services that are being updated include the B2B Web Service Gateway and Electronic Document Interchange Gateway, Passage Services, and Secondary Processing and Passage History (SPPH) to include the electronic declaration data stored as part of the passage record. The role of each impacted service is demonstrated in Diagram 5 in Section 4.1.

This initiative requires the collection of a photo of the individual's face and the use of facial authentication software to compare the visual image to the image on the travel document. For travellers without an ePassport, a CBSA officer will complete a manual authentication, to ensure the traveller image captured at the kiosk matches the individual presenting the receipt.

Data linkages will be established with other CBSA information holdings to validate and verify the information provided by the traveller. These data linkages are already in place to support primary processing at traditional Primary Inspection Line – the PIK will simply automate the queries and validation of information, replacing the need for a CBSA officer to manually complete this task.

Personal Information Transmission

Level of Risk

The personal information is used within a closed system.

No connections to Internet, Intranet or any other system. Circulation of hardcopy documents is controlled.

☐ 1

The personal information is used in system that has connections to at least one other system.

☒ 2

Primary Inspection Kiosk	PIA
The personal information is transferred to a portable device or is printed. USB key, CD-Rom, laptop computer, any transfer of the personal information to a different medium.	<input checked="" type="checkbox"/> 3
The personal information is transmitted using wireless technologies.	<input type="checkbox"/> 4
Details: Requirements for the kiosk set up, configuration, connection and routing of information are part of a Service Level Agreement between the Airport Authority and the CBSA. No kiosk will be activated until the CBSA has confirmed it meets the requirements specified; before activation, the CBSA must issue a digital certificate to each kiosk, to digitally sign the SOAP message for identity verification and integrity of the message, which ensures information has not been altered from what was collected at the Kiosk. Each kiosk will create a secure (encrypted) TLS connection (HTTPS) to the CBSA reverse proxy server to ensure confidentiality of the information exchange. All traffic generated from the kiosk to the CBSA will be routed over the Internet through a managed and encrypted VPN connection to also ensure additional confidentiality and isolation of the message traffic over the Internet. All kiosks messages are authenticated through SiteMinder technology and then provided authorization to access PIK Services deployed on the CBSA Secure Cluster as well as supporting services deployed in the CBSA operational restricted zone. Diagram 6 in Section 4.1 address information transmission.	

Risk Impact to the CBSA	Level of Risk
Managerial harm. Processes must be reviewed, tools must be changed, change in provider / partner.	<input type="checkbox"/> 1
Organizational harm. Changes to the organizational structure, changes to the organizations decision-making structure, changes to the distribution of responsibilities and accountabilities, changes to the program activity architecture, departure of employees, reallocation of HR resources.	<input type="checkbox"/> 2
Financial harm. Lawsuit, additional moneys required reallocation of financial resources.	<input type="checkbox"/> 3
Reputation harm, embarrassment, loss of credibility. Decreased confidence by the public, elected officials under the spotlight, institution strategic outcome compromised, government priority compromised, impact on the Government of Canada Outcome areas.	<input checked="" type="checkbox"/> 4

Details: In the event of a breach of the personal information collected and transmitted by the PIK, there would be a decrease in public confidence regarding the CBSA's ability to responsibly handle personal information. The Service Level Agreement, initiative design, systems architecture and configuration requirements provide an adequate level of protection to mitigate this risk. Given the safeguards in place, moving to electronic collection of data represents a lower risk than the manual collection of data using the legacy paper declaration forms.

Risk Impact to the Individual or Employee

Level of Risk

Inconvenience.	<input checked="" type="checkbox"/> 1
Reputation harm, embarrassment.	<input checked="" type="checkbox"/> 2
Financial harm.	<input checked="" type="checkbox"/> 3
Physical harm.	<input type="checkbox"/> 4

Details: In the event of a breach of passport / travel personal information collected and transmitted by the PIK, there could be the possibility of identity theft of the individual. Again, the Service Level Agreement, initiative design, systems architecture and configuration requirements provide an adequate level of protection to mitigate this risk.

Primary Inspection Kiosk

PIA

SECTION 3 - ANALYSIS OF PERSONAL INFORMATION ELEMENTS

Personal Information Elements and Sub-elements - Kiosk

The following table lists the personal information elements collected via PIK.

Note: A separate table, which follows, reflects the information elements captured by the CanBorder-eDeclaration app.

Category Of Personal Information	Personal Information Element	Personal Information Sub-Element	Format	Source	Purpose / Necessity of Element
Name	1) Name	1) Last name, first name, middle initials	Electronic	Derived from the travel document at the kiosk	To document border crossing; identify travellers in existing CBSA information holdings and assess admissibility.
Province/Country Information	1) Partial Address	1) Country 2) Province (for residents of Canada) 3) State (for residents of the U.S.)	Electronic	Traveller data entry at kiosk	To document border crossing; identify travellers in existing CBSA information holdings and assess admissibility. Place of residence is also used to determine which additional customs related questions are asked to a traveller (i.e., defines resident vs. non-resident).
Biometric	1) Visual image	1) Visual image of the traveller, taken by the kiosk. (Note: visual images are only captured for travellers that are 14 years of age and older.)	Electronic	Photo capture at the kiosk	To authenticate that the client in front of the kiosk corresponds with the individual's photo embedded in the chip of their ePassport chip (for the clients that have this feature in their passport). For all clients, the photo will be printed on the kiosk receipt as a means of connecting the individual(s) with their declaration throughout the rest of the CBSA service area. CBSA officers will manually authenticate that the individual(s) presenting the receipt are those featured in the photos. This will improve traveller flow, strengthen travellers' identity reconciliation,
Citizenship / Nationality	1) Citizenship / Nationality	1) Citizenship / nationality of traveller	Electronic	Derived from the travel document at the kiosk	To document border crossing; identify travellers in existing CBSA information holdings and assess admissibility.
Purpose of Trip	Purpose of trip	1) Personal 2) Study 3) Work or Employment 3) Immigrate	Electronic	Traveller data entry at kiosk	To assess admissibility of foreign national travellers.
Date of birth	Date of birth	1) Day of birth 2) Month of birth 3) Year of birth	Electronic	Derived from the travel document	To identify travellers in existing CBSA information holdings and assess admissibility.

Primary Inspection Kiosk

PIA

Gender	Gender	Gender of Traveller	Electronic	Derived from the travel document	To identify travellers in existing CBSA information holdings and assess admissibility.
Travel Document Information (may be their Passport)	1) Travel Document Information	1) Document Type 2) Document Number 3) Document Country of Issuance 4) Document expiration date 5) Public Key Directory (PKD)	Electronic	Derived from the travel document	To document border crossing; identify travellers in existing CBSA information holdings and assess admissibility; to verify the validity and authentication of the travel document. In the past, a CBSA officer would manually verify the travel document; through PIK, the kiosk will conduct these tasks, validating the document against PKD information.
Customs and OGD Related Questions	Declaration questions	Declaration questions related to: 1) Firearms or other weapons 2) Commercial goods 3) Food, plant or animals 4) Currency (more than \$10,000) 5) Unaccompanied goods 6) Visit to a farm abroad and destined to a farm in Canada Declaration related to personal exemption (returning residents) and allowance (visitors); and value of goods for travellers indicating they exceeded their exemption limit.	Electronic	Traveller data entry at kiosk	To assess duties and taxes; to assess goods admissibility.
Duration of stay in Canada	Duration of stay in Canada	Duration of stay in Canada	Electronic	Traveller data entry at kiosk	To assess admissibility of foreign national travellers.
Duration of stay outside of Canada	Duration of stay outside of Canada	Duration of absence from Canada	Electronic	Traveller data entry at kiosk	To assess traveller exemption allowance for Canadian residents
Signature	Electronic Signature	Physical signature replaced by on-screen confirmation that the declaration is true, accurate and complete.	Electronic	Traveller data entry at kiosk	Validation of the information provided.

Personal Information Elements and Sub-elements – eDeclaration

Primary Inspection Kiosk

PIA

The following table lists the personal information elements collected via the CanBorder-eDeclaration app. It is important to note that the app provides travellers an opportunity to complete their declaration in advance of arrival; however, it has been deliberately designed to capture the minimum information required to that of a non-sensitive nature. Travellers are identified solely by nicknames within the app. At the kiosk, each traveller will be prompted by nickname to scan their travel document and present for a photo, reconciling the declaration stored within the QR code, with their legal name. No information is transmitted to the CBSA in advance of arrival as there is no connection between the mobile application and the CBSA's systems. Each traveller declaration will be reconciled with a travel document scan and photo at the kiosk proper. Additionally, app users will have the opportunity to review and edit their declaration on the kiosk, improving data validity and ensuring every opportunity to make a full and complete declaration.

Category Of Personal Information	Personal Information Element	Personal Information Sub-Element	Format	Source	Purpose / Necessity of Element
Province/Country Information	1) Partial Address	1) Country 2) Province (for residents of Canada) 3) State (for residents of the U.S.)	Electronic	Traveller data entry on the app.	To document border crossing; identify travellers in existing CBSA information holdings and assess admissibility. Place of residence is also used to determine which additional customs related questions are asked to a traveller (i.e., defines resident vs. non-resident).
Purpose of Trip	Purpose of trip	1) Personal 2) Study 2) Work or employment 3) Immigrate	Electronic	Traveller data entry on the app.	To assess admissibility of foreign national travellers.
Customs and OGD Related Questions	Declaration questions	Declaration questions related to: 1) Firearms or other weapons 2) Commercial goods 3) Food, plant or animals 4) Currency (more than \$10,000) 5) Unaccompanied goods. 6) Visit to a farm abroad and destined to a farm in Canada. Declaration related to personal exemption (returning residents) and allowance (visitors); and value of goods for travellers indicating they exceeded their exemption limit.	Electronic	Traveller data entry on the app.	To assess duties and taxes; to assess goods admissibility.

Continued

Duration of stay in Canada	Duration of stay in Canada	Duration of stay in Canada	Electronic	Traveller data entry on the app.	To assess admissibility of foreign national travellers.
Duration of stay outside of Canada	Duration of stay outside of Canada	Duration of absence from Canada	Electronic	Traveller data entry on the app.	To assess traveller exemption allowance for all Canadian residents.
Signature	Electronic Signature	Physical signature replaced by on-screen confirmation that the declaration is true, accurate and complete.	Electronic	Traveller data entry on the app.	Validation of the information provided. App users will review their full declaration before generating their QR code and will be presented with an editable summary at the kiosk for final confirmation.

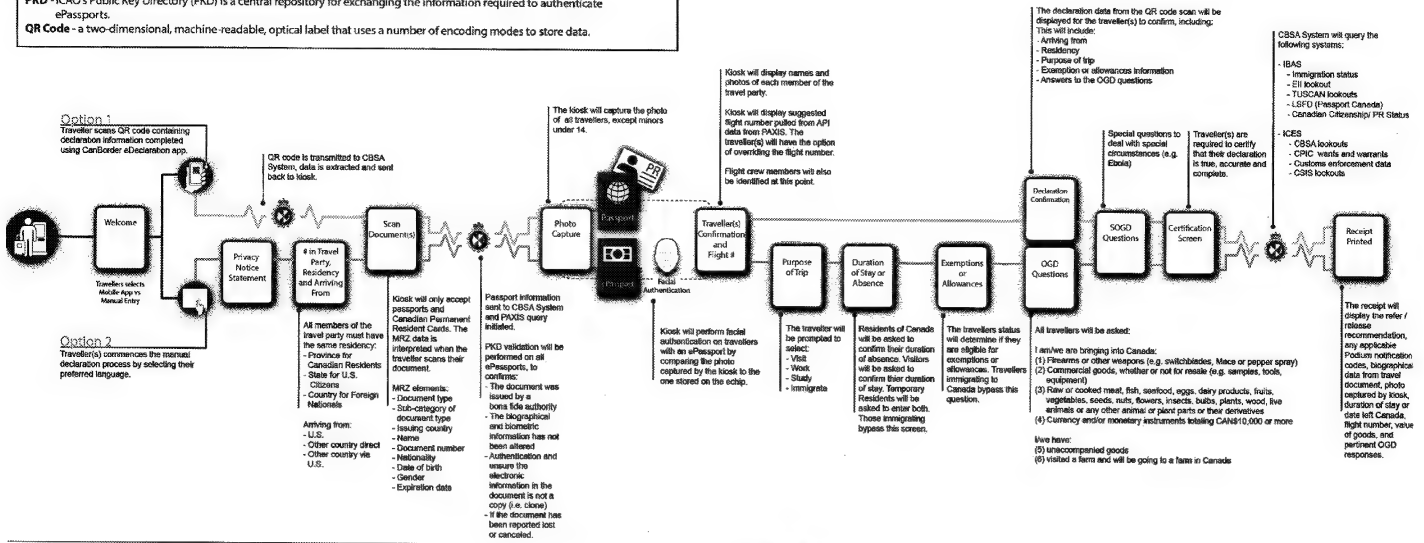
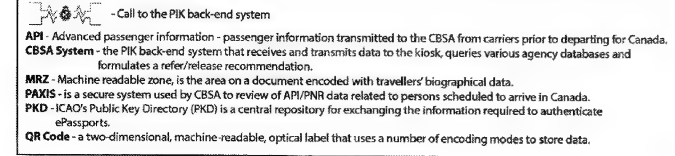
Primary Inspection Kiosk

PIA

SECTION 4 - FLOW OF PERSONAL INFORMATION

4.1 Data Flow Model - Diagram

Diagram 1 – Legend



Primary Inspection Kiosk

PIA

Data Elements Exchanged between Kiosk and CBSA during Traveller Session

Message	Origin of Data	Destination	Data and Context	Personal Traveller Data?	Comments	Data Element Stored in CBSA System
Kiosk Message #1	Kiosk	PIK Service	Kiosk Identifier	No	Kiosk will capture and send Biographic and initial Declaration Data to CBSA for pre-processing & eligibility to use Kiosk.	Yes - ICS
			Selected Language	No		Yes - ICS
			Travel Document MRZ	Yes		Yes - ICS
			Includes Name, Nationality, DOB, Gender			
getFlightData	PIK Service	PAXIS	Surname	Yes	Surname of traveller	Yes - PAXIS
			First Name	Yes	First Name of traveller	Yes - PAXIS
			Date of Birth	Yes	Date of Birth of traveller	Yes - PAXIS
			Document Number	Yes	Travel document number	Yes - PAXIS
	PAXIS	PIK Service	Name	Yes	Combined Name of traveller	Yes - ICS
			Date of Birth	Yes	Date of Birth of traveller	Yes - ICS
			Document Number	Yes	Travel document number	Yes - ICS
			Port of Departure	No	Port of Departure	Yes - ICS
			Port of Arrival	No	Port of Arrival	Yes - ICS
			Flight Number	No	Flight Number	Yes - ICS
			Carrier Code (IATA)	No	Carrier Code (IATA)	Yes - ICS
			Carrier Code (ICAO)	No	Carrier Code (ICAO)	Yes - ICS
			Code Share List	No	Code Share List	Yes - ICS
			Passenger Type (Crew Indicator)	No	Passenger Type (Crew Indicator)	Yes - ICS
			Flight ID	No	PAXIS Flight identifier	Yes - ICS
			PAXIS Traveller ID *only if traveller is found	Yes	PAXIS Traveller Identifier	Yes - ICS

Primary Inspection Kiosk

PIA

Result	PIK Service	Kiosk	Eligibility code	No	PIK Service will return a success indicator if traveller is eligible to use the Self Service kiosk, as well as flight data found for the traveller and the dynamic OGD/SOGD question set in their chosen language.	N/A
			Flight Number			N/A
			Dyanamic OGD/SOGD question set in chosen language.			N/A
						N/A

Kiosk Message #2	Kiosk	PIK Service	Kiosk Identifier	No	Unique identifier for the Kiosk	Yes - ICS
			Selected Language	No	Chosen language to be displayed on all kiosk screens	Yes - ICS
			Privacy Acknowledged	No	Indicator that the privacy disclaimer was agreed to	Yes - ICS
			Mobile App used Ind.	No	Indicator if mobile eDeclaration presented to kiosk to initiate the Kiosk session.	Yes - ICS
			# of travellers in group	No	Number of travellers in group	Yes - ICS
			Declaration Certified Ind.	No	Indicator that the declaration was certified by the traveller	Yes - ICS
			Place of Residence	No	Country and Prov/State only	Yes - ICS
			Flight Number	No	The flight number returned from CBSA based on pre-arrival data supplied by air carriers.	Yes - ICS
			Manual Flight Number Entered	No	If no flight was returned from CBSA, or there was a manual correction made to the flight number by the traveller.	Yes - ICS
			Arriving From	No	US Direct, International, Other.	Yes - ICS
			Travel Document MRZ	Yes	Biographic Data including Name, Nationality, DOB, Gender.	Yes - ICS

Primary Inspection Kiosk

PIA

			ePassport Chip Data	Yes	Biographic and Photo encoded on the ePassport chip.	No
			Declaration Data - Purpose of trip, duration of stay, duration of absence, value of goods, answers to OGD/SOGD questions.	No	Declaration Data includes answers to declaration questions, including OGD/SOGD equivalent to E311 data.	Yes - ICS
			Traveller Photo	Yes	Live photo taken at Kiosk.	No
			Facial match result	No	The Kiosk is responsible to conduct facial matching of the live photo against the ePassport photo, and supply the matching results calculated by the Kiosk.	Yes - ICS
Validate Travel Document	PIK Service	Travel Document Verification Service (TDVS)	Travel Document MRZ	Yes	Internal to CBSA, Biographic Data and Photo is delivered to backend service that verifies the travel document is valid and has not been tampered with by verifying the digital signature against ICAO's PKD.	No
			ePassport Chip Data (if ePassport)			No
	TDVS	PIK Service	Travel Document MRZ	Yes	The MRZ String being verified	Yes - ICS
			Verification Result	No	Trust level of the validation result (1-7)	Yes - ICS
			Result Reason	No	Description of the trust level reasons	Yes - ICS
Perform Risk Assessment	PIK Service	IBAS (through Passage	Travel Document Number	Yes	Travel Document Number	No

Primary Inspection Kiosk

PIA

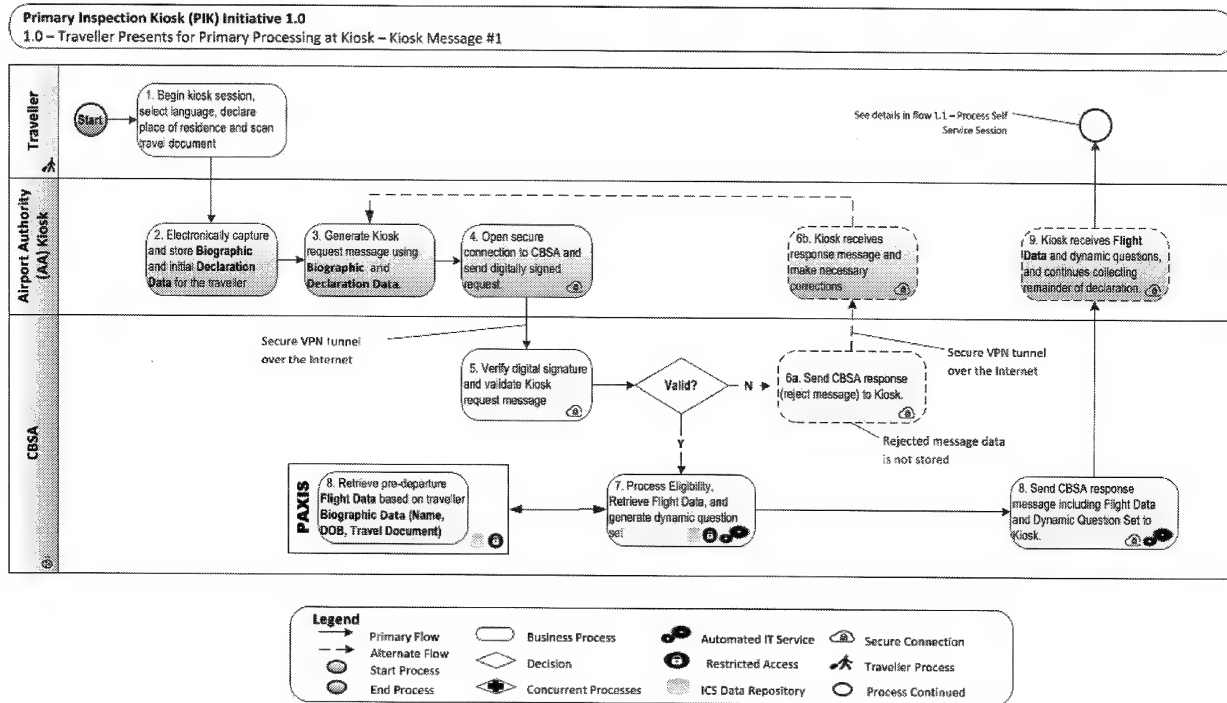
	Services - CQ	Traveller Name	Yes	Surname, Given Name	No
IBAS	PIK Service	Given Names	Yes	Traveller Biographic Data, as stored in IBAS (from IRCC, GCMS System)	Yes - ICS
		Surname			
		Gender			
		DOB Day			
		DOB Month			
		DOB Year			
		Country of Birth			
		Citizenship			
		Serial Number	Yes	IRCC generated data, representing Immigration Permit Data	Yes - ICS
		IdType			
		CounterfoilCategory			
		CounterfoilEntryType			
		IssueDate			
		ExpiryDate			
		Country			
		Status			
PIK Service	ICES (through Passage Services - CQ)	Travel Document Number	Yes	Travel Document Number	No
		Traveller Name	Yes	Surname, Given Name(s)	No
ICES	PIK Service	Given Names	Yes	Traveller Biographic Data, as stored in ICES	Yes - ICS
		Surname			
		Gender			
		DOB			

Primary Inspection Kiosk

PIA

			Previous Enforcement Actions	Yes	A list of previous enforcement actions taken against the traveller	Yes - ICS
			Lookout indicators	Yes	An indicator if the traveller has a lookout created, by lookout type.	Yes - ICS
			Percentage Match Indicator	No	A confidence percentage match between name supplied and ICES record.	No - Generated
Result	PIK Service	Kiosk	Response Code	No	A Success or failure indicator for the self-service session result.	Yes - ICS
			Receipt	Yes	Biographic data and Photo captured at kiosk as well as Travel Document Number and CBSA referral codes are printed on the receipt.	Yes - ICS (CBSA copy of generated receipt)

Diagram 2 –



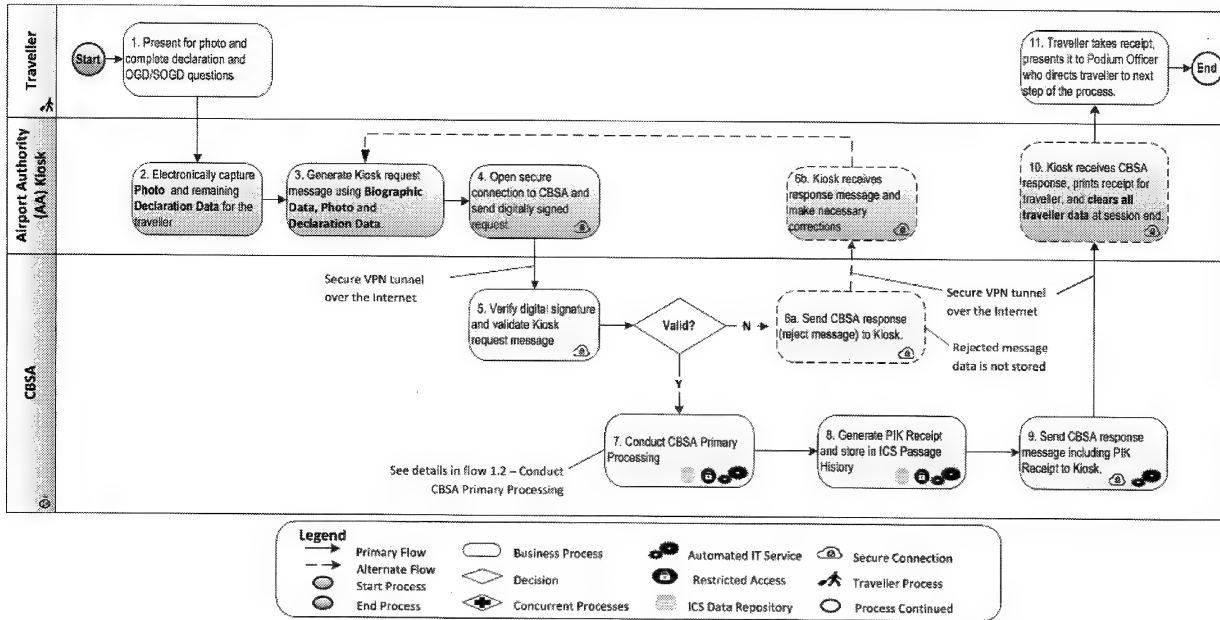
Primary Inspection Kiosk

PIA

Diagram 3 –

Primary Inspection Kiosk (PIK) Initiative 1.0

1.1 – Perform Primary Processing Assessment of Traveller – Kiosk Message #2



Primary Inspection Kiosk

PIA

Diagram 4 –

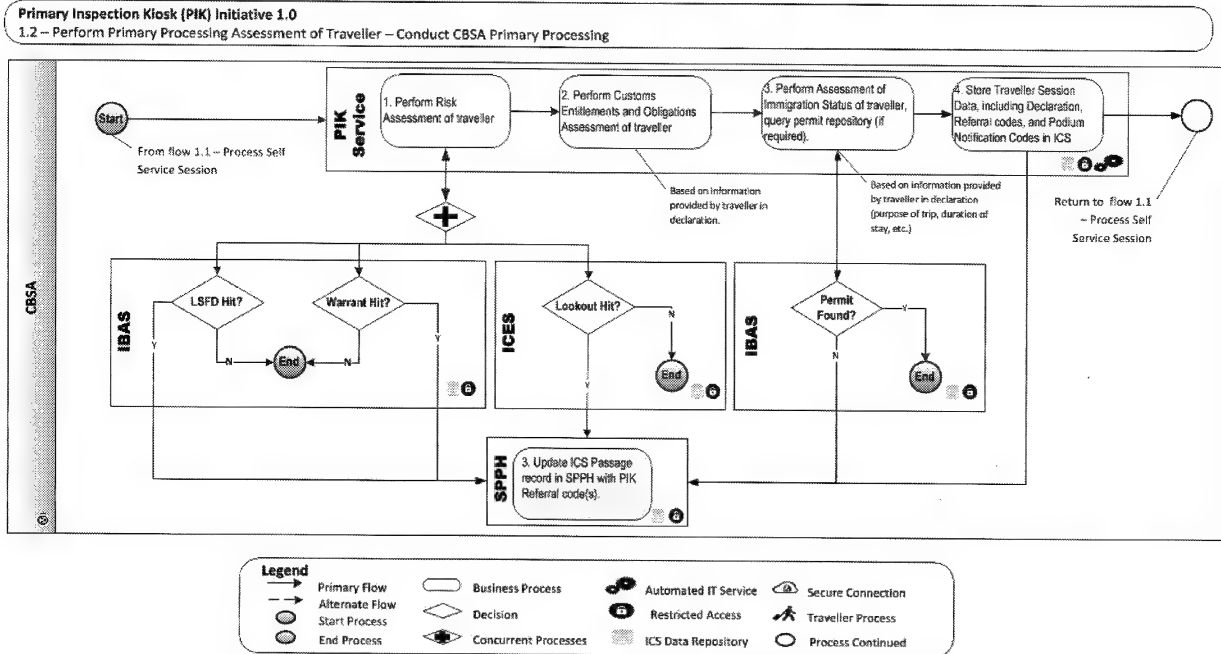
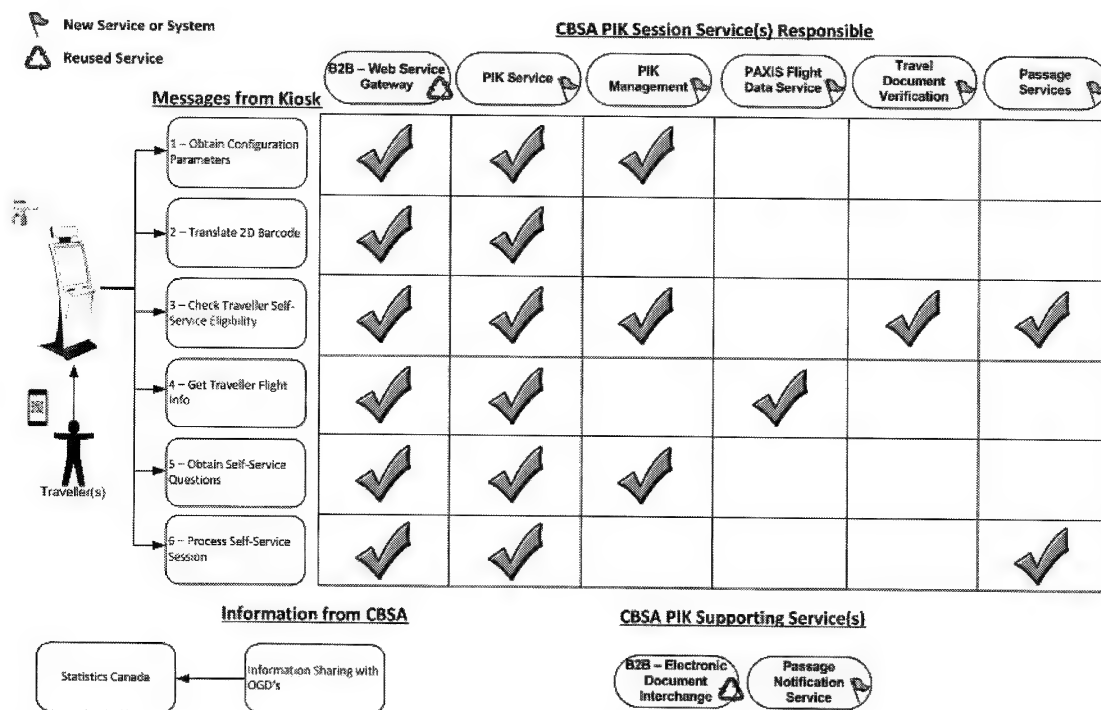


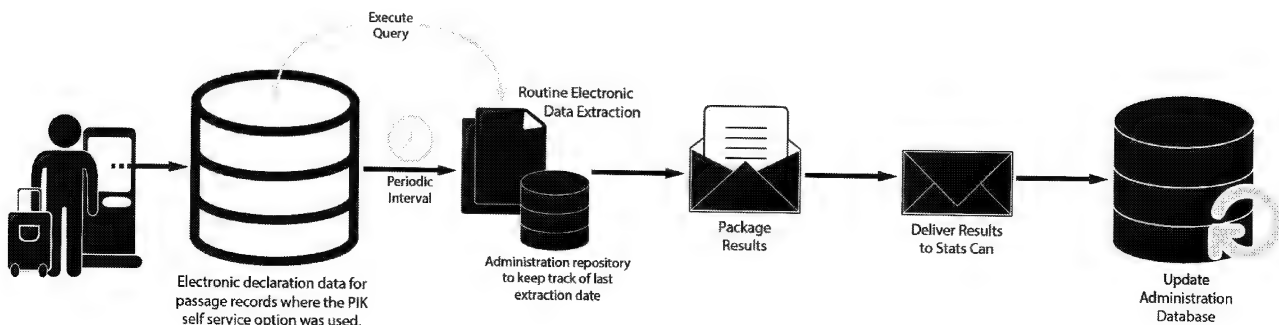
Diagram 5 -



Primary Inspection Kiosk

PIA

Diagram 7 –



Traveller data elements collected through PIK and to be shared with StatCan:

First Name	Purpose of trip (foreign nationals only)
Last Name	Duration of stay (visitors)
Language selected	Duration of absence from Canada (residents):
Document type	-24 Hours or less
DOB	-More than 24 hours but less than 48 hours
Citizenship	-More than 48 hours but less than 7 days
Gender	-7 days or more
Province / State / Country	Arriving by
Airline Code/Conveyance number	Arriving from
Crew Y/N	Number of people in session

4.2 Data Flow Model - Table

SOURCE	IDENTIFY THE SOURCE
The individual or a representative	Traveller
CBSA Information Holdings	<p>CBSA Information holdings such as:</p> <ul style="list-style-type: none"> Integrated Customs System (ICS): A common platform for managing authorized and authenticated access to the CBSA systems: <ul style="list-style-type: none"> PIK Service - that handles the orchestration and coordination of primary processing for each traveller using the self-service Kiosk option. Secondary Processing and Passage History (SPPH) to store traveller encounters, including declaration data, referral codes, and examination results. Passenger Information System (PAXIS) to retrieve passenger and flight information through the Advance Passenger Information (API) – CBSA PPU 008. Integrated Custom Enforcement System (ICES) – CBSA PPU 016. Data from the following programs is accessed through ICES: <ul style="list-style-type: none"> Criminal Investigation Program – CBSA PPU 1402; and Intelligence Program – CBSA PPU 035. Interdiction and Border Alert System (IBAS). Data from the following programs/systems is retrieved through IBAS: <ul style="list-style-type: none"> Immigration Investigations Program – CBSA PPU 1403 Enforcement Information Index System (EIIS) – CBSA PPU 025 Document Integrity Program – CBSA PPU 1404 <p>The Lost Stolen Fraudulent Document (LSFD). *Immigration related data is retrieved from Global Case Management System (GCMS) through IBAS.</p>
Royal Canadian Mounted Police Information Holdings	A subset of Wants and Warrants from Canadian Police Information Centre (CPIC) is sent to ICES (CBSA PPU 016).

4.3 Internal Use and Disclosure

Program	Personal information bank
Secondary Processing	Traveller Processing PIB CBSA PPU 1101

4.4 External Use and Disclosure

The individual or a representative	
A federal government institution	Statistics Canada, as per the terms of the current Memorandum of Understanding and an Annex (being drafted), supporting the sharing of information collected by the CBSA. Disclosure authority under Section 107(5)(b) of the <i>Customs Act</i> .
	Public Health Agency of Canada, Traveller Illness Reports PHAC PPU 071, as per existing information sharing agreements, upon request when required to support national health and safety. Disclosure authority under Section 107(4)(e) or 107(5)(b) of the <i>Customs Act</i> .
	Employment and Social Development Canada, Employment Benefits, Support Measures and Other Programs ESDC PPU 293. The data elements collected through PIK to be shared with ESDC and the authorities are being reviewed.
Non-federal institutions and private sector	
- Provincial Government	No systematic disclosures; any disclosures would be pursuant to Section 8(2) of the <i>Privacy Act</i> and/or Section 107 of the <i>Customs Act</i>
- Municipal Government	No systematic disclosures; any disclosures would be pursuant to 8(2) of the <i>Privacy Act</i> and/or Section 107 of the <i>Customs Act</i>
- Aboriginal Government / Council	No systematic disclosures; any disclosures would be pursuant to 8(2) of the <i>Privacy Act</i> and/or Section 107 of the <i>Customs Act</i>
- Organization of a Foreign State	No systematic disclosures; any disclosures would be pursuant to 8(2) of the <i>Privacy Act</i> and/or Section 107 of the <i>Customs Act</i>
- International Organization	No systematic disclosures; any disclosures would be pursuant to 8(2) of the <i>Privacy Act</i> and/or Section 107 of the <i>Customs Act</i>
Private Sector	
- Located in Canada and Canadian Owned	None
- Located in Canada and Foreign Owned	None
- Located abroad and Canadian Owned	None
- Located abroad and Foreign Owned	None

Disclosure of the personal information collected is communicated in the privacy notice statement provided to users at the point of collection, either on the mobile device or at the kiosk, which mirrors the CBSA's existing processes for

information collected via the E311. While risks inherent in the other organizations cannot be mitigated by the CBSA, it is possible that the CBSA can influence the transparency of the process.

The following section examines privacy compliance (at a high level) for the transparency of the disclosure of information to StatCan, as included in this initiative. The disclosure of information to any other government departments, per existing agreements, is not further explored in this PIA, as there are no changes to the established processes.

Statistics Canada

The external disclosure of E311 information to StatCan enables the digitization of the information (by StatCan) and is used to validate the findings of their International Travel publication. Though 2015 demographic information is available online for manipulation, the last International Travel publication located on line is from 2010. In 2010, StatCan received and processed 18.3 million E311 traveller declaration cards. The information used to populate the report is collected via a questionnaire handed out to travellers, then validated by the information captured in the E311. The survey results may be impacted by two types of bias: distribution bias could result if only specific types of people are given questionnaires and non-response bias could result if only specific types of people actually respond to the questionnaire. In order to improve the accuracy of the data, StatCan pulls a sample of the E311 cards, filled in by the responsive travellers. Questionnaire responses for trip purpose and duration of trip are compared to the responses received on the questionnaire.⁴

The collection, digitization and use of the information are not clearly reflected in an institution-specific Personal Information Bank, published in Info Source by StatCan. Discussions with StatCan privacy personnel iterate that the information is not used to make any administrative decisions that directly affect the individual and is not stored in a manner that would make the information realistically retrievable, in the event of a request for access. While the individual's information could be located within the digital records, it would not be likely that the information could be reasonably located within the almost 20 million records.

For this reason, StatCan represents the collection in Classes of Records: Tourism Statistics (StatCan ETC 180) and represents the process of collection / digitization in a high level description, "5.4) Cost-recovered Services related to Statistical Infrastructure."

Within the published report, there are references to the use of the CBSA E311 card. There are, however, no transparent references to the collection and use of the E311 card communicated to the public in the StatCan information holdings.

There is a Memorandum of Understanding in place between the CBSA and StatCan, which includes the personal information collected through traveller processing. In digitizing the print records, StatCan required access to the entire E311 document. With PIK, the records will be digital at the point of collection, so StatCan will not be required to scan the E311 cards. They will, however, continue to complete some statistical analysis on the data for the CBSA. As part of the PIK initiative, a review of the existing information sharing practices and personal information elements required for both traveller processing and statistical analysis was conducted. In doing so, the CBSA validated the data to be shared and has confirmed that only the elements required will be disclosed. Section 107(5)(b) of the *Customs Act* provides the authority for the disclosure. An Annex to the current Memorandum of Understanding with StatCan is being drafted to reflect the data to be shared and transmission process.

(See Diagram 7 in Section 4.1 for flow of information from PIK to CBSA to StatCan and traveller data elements collected through PIK to be shared with StatCan).

⁴ Statistics Canada Report, International Travel 2010, page 58.

4.5 Retention / Storage

Canada Border Services Agency - Integrated Customs System (ICS), Passage History database	<p>Files are retained for seven years from the date of the traveller's entry to Canada, as identified by the traveller's passage time, recorded at the kiosk. This reflects existing retention periods for traveller processing. After this period, the records are destroyed.</p> <p>No personal data is retained by the kiosk. Data collected during the traveller processing is erased from the kiosk in a way to make it irretrievable on completion of the traveller's passage event.</p>
---	--

4.6 Other Possible Considerations

Identify Groups or Areas / or Divisions	Positions who have access or use the personal information (where appropriate)	Geographical Location
The CBSA responsible for program or activity:		
Traveller Transformation Directorate	Approximately 25-50 staff members	National Capital Region
Information, Science and Technology Directorate	Approximately 20-25 staff members in a production support role, responsible for receiving incidents and requests from end-users, analyzing these and either responding to the end user with a solution or escalating it to the other IT teams. These teams may include developers, system engineers and database administrators handling system issues	National Capital Region
Border Operations Directorate	Approximately 1750 staff members including Border Services Officers, interns/students, Superintendents, Chiefs of Operations	Top ten Canadian airports – Toronto, Ottawa, Vancouver, Calgary, Edmonton, Winnipeg, Montreal, Halifax, Billy Bishop and Quebec City
Recourse Directorate	Approximately 25-30 staff members handling recourse and appeals	National Capital Region and Regional Offices
Other federal government Institution responsible for program or activity:		
Statistics Canada	StatCan estimates access is limited to 50 staff members, including scanning clerks and statisticians	National Capital Region

SECTION 5 - PRIVACY COMPLIANCE ANALYSIS

1. Legal Authority for Collection of Personal Information

Has a legal authority been identified for the collection of personal information for this program or activity?

Yes

- 1.1 ☒ Specify the legal authority and briefly explain its connection to the program or activity or how it permits the collection of the personal information:

Legal authority for the collection of personal information via the print E311 and through the automated primary inspection process facilitated through the PIKs is derived from multiple, inter-related legislations and regulations.

- Information required for the regulation of goods (import/export) is derived from one legislation and supporting regulations. 1) Section 12 of the *Customs Act*, which states, "all goods that are imported shall, except in such circumstances and subject to such conditions as may be prescribed, be reported at the nearest customs office designated for that purpose that is open for business." And 2) Section 5(3) of the *Reporting of Imported Goods Regulations*, which states, "Goods that are imported by a person arriving in Canada on board a commercial passenger conveyance other than a bus shall be reported in writing."
- Information required from individuals as they request entry into Canada is derived from two legislations. 1) Section 11 of the *Customs Act*, which states, "every person arriving in Canada shall, except in such circumstances and subject to such conditions as may be prescribed, enter Canada only at a customs office designated for that purpose that is open for business and without delay present himself or herself to an officer and answer truthfully any questions asked by the officer in the performance of his or her duties under this or any other Act of Parliament." And 2) Section 18(1) of the *Immigration and Refugee Protection Act* which states, "Every person seeking to enter Canada must appear for an examination to determine whether that person has a right to enter Canada or is or may become authorized to enter and remain in Canada."

In addition to these specific legal authorities, information is also collected under the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, as well as associated regulations made thereunder such as the *Cross-border Currency and Monetary Instruments Reporting Regulations*. Subsection 12(1) of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* states, "every person or entity referred to in subsection (3) shall report to an officer, in accordance with the regulations, the importation or exportation of currency or monetary instruments of a value equal to or greater than the prescribed amount."

Program legislation as defined in the Customs Act “means any other Act of Parliament or any instrument made under it, or any part of such an Act or instrument,

(a) that the Governor in Council or Parliament authorizes the Minister, the Agency, the President or an employee of the Agency to administer and enforce, including the Customs Act, the Customs Tariff, the Excise Act, the Excise Act, 2001, the Immigration and Refugee Protection Act and the Special Import Measures Act;

(b) that the Governor in Council or Parliament authorizes the Minister, the Agency, the President or an employee of the Agency to enforce, including the Agriculture and Agri-Food Administrative Monetary Penalties Act, the Canada Agricultural Products Act, the Feeds Act, the Fertilizers Act, the Fish Inspection Act, the Health of Animals Act, the Meat Inspection Act, the Plant Protection Act and the Seeds Act;

(c) under which the Minister or another minister authorizes the Agency, the President or an employee of the Agency to administer a program or carry out an activity; or

(d) under which duties or taxes collected and paid pursuant to the Customs Act are imposed.”

- 1.3 ☒ Is the personal information collected directly related to an operating program or activity?

Details: the information collected has been cross-referenced with the purpose of collection.

No

- 1.3 ☐ If there is no legal authority for the collection of personal information, it cannot be collected. Please consult your legal advisor to determine if there is authority to proceed with the program or activity.

2. Necessity to Collect Personal Information

Is each element and sub-element of personal information collected or to be collected necessary to administer the program or activity?

YES

- 2.1 ☒ Ensure that all personal information necessary to administer the program or activity is listed in the relevant **PIB**.
- 2.2 ☒ AND, implement controls and procedures to ensure the CBSA does not collect more personal information than is necessary for the identified program or activity and that a continuing need exists for that information or its collection.

2.3 Are secondary uses contemplated for the information collected?

☒ YES ☐ NO

The use of the information for enforcement (if required) internal to the CBSA and disclosures to other government departments such as StatCan would be considered secondary uses. These uses are documented in the Personal Information Bank and notice is provided to the individual at the point of collection.

2.3.2 If not, is there authority for the use or disclosure of the personal information?

☒ YES ☐ NO

NO

- 2.3 ☐ Review the proposed elements and sub-elements of personal information outlined in "Section 3 – Analysis of Personal Information Elements" to identify those that are "necessary" and not merely useful. Document any changes.

3. Authority for the Collection, Use or Disclosure of the Social Insurance Number

Is the collection of the Social Insurance Number (SIN) necessary to administer the program or activity?

YES

- 3.1 ☐ Collection of the SIN must be in compliance with the *Directive on Social Insurance Number* (please check all appropriate boxes below):

- 3.2 ☐ State legal authority for collecting the SIN:

OR, in the absence of a legal authority to collect the SIN:

- 3.3 ☐ Establish explicit authority through legislative amendment(s).
 3.4 ☐ Establish legal authority as outlined in the *Directive on Social Insurance Number*.

AND, if disclosure of the SIN by the CBSA is to occur on a routine or systematic basis

- 3.4.1 ☐ to another federal institution that is authorized to collect it, or to another level of government, establish an agreement or arrangement that includes specific provisions to limit the use of the SIN.
 3.4.2 ☐ to a contractor or other external service provider, establish a contract that includes specific provisions to limit the use of the SIN.
 3.5 ☐ AND, ensure that the relevant **PIB** for the program or activity states the authority under which the SIN is collected and the purpose for which it is used.

NO

- 3.6 ☒ The SIN is not necessary and it will not be collected, used or disclosed to administer the program or activity.

4. Direct Collection - Notification and Consent (as appropriate)***Is personal information collected directly from the individual to whom it relates?*****YES**

- 4.1 ☒ A "**Privacy Notice**" (adapted for either verbal or written communications) must be provided to the individual at the time of collection and it must include the following elements:
- a) The purpose and authority for the collection
 - b) Any uses or disclosures that are consistent with the original purpose.
 - c) Any uses or disclosures that are not related to the original purpose
 - d) Any legal or administrative consequences for refusing to provide the personal information
 - e) That the "individual to whom the information relates" has rights of access to, correction of and protection of personal information under the *Privacy Act*.
 - f) A reference to the **PIB** for the program or activity
 - g) Why the SIN is collected, how it will be used and the consequence of not providing it.

AND, add a "**Consent Statement**" to the "**Privacy Notice**" as appropriate, if the personal information is to be used or disclosed for a purpose other than the original purpose (**Secondary Use**) or a consistent use, or, to authorize indirect collection of personal information.

- 4.2 ☐ The "**Consent Statement**" must include the following elements:
- a) The purpose of the consent and the specific personal information involved.
 - b) In the case of indirect collections, the sources that will be asked to provide the information. (This element need only be included when personal information is to be collected from another source e.g., person or organization with the consent of the individual)
 - c) Uses and disclosures that are not consistent with the original purpose of the collection and for which consent is being sought.
(This element need only be included when the individual's consent is sought for a secondary use or disclosure that is not consistent with the original purpose for which the information is collected. To find out if the individual's consent is necessary for such a use or disclosure, please consult the ATI and Privacy Division)
 - d) Any consequences that may result from withholding consent.
 - e) Any alternatives to providing consent

- 4.3 ☐ AND, implement controls and procedures to ensure that the CBSA keeps a record documenting whether or not an individual provided consent when it was sought, including a record documenting any withdrawal of consent when applicable.

****Ensure to provide the "controls and procedures" as an annex to this PIA****

Additional Consent Considerations (s. 77(1)(m) of the *Privacy Act*):

- ☐ Standards and mechanisms are in place to ensure that the individual has capacity to give consent.

****Ensure to provide the "standards and mechanisms" as an annex to this PIA****

There will be a Privacy Notice Statement on kiosk and the eDeclaration app, which all travellers will be required to acknowledge. In order to be compliant with the requirements of the Directive on Privacy

Practices, the Privacy Notice Statement for the kiosk and the app reflect the individual's right to complain to the Office of the Privacy Commissioner. Additionally, the CBSA has incorporated OPC feedback concerning the E311 and ABC Privacy Notice Statement. The Privacy Notice Statements for the kiosk and the eDeclaration mobile app were drafted to ensure they are clear and complete.

The **Privacy Notice Statement for the kiosk** covers the disclosure of information while using the kiosk only (see Annex B for full text). The **Privacy Notice Statement for the app** covers the disclosure of information while using the app and the kiosk (see Annex C for full text).

NO

- 4.4 ☐ The personal information necessary for the program or activity is not collected directly from the individual. It is collected indirectly, for example, from another program within the CBSA, or from another institution, government or third party.

5. Indirect Collection - Consent or Authority under Sec. 10 of Privacy Regulations

Is personal information collected indirectly from another source with the informed consent of the individual to whom it relates, or from a person authorized to act on behalf of the individual pursuant to section 10 of the Privacy Regulations?

YES

- 5.1 ☐ The notice and consent requirements stated at Question 4 apply. Please provide the "**Privacy Notice**" and/or "**Consent Statement**" below:

****For a copy of the CBSA Privacy Notice and Consent Statement template, contact the ATI and Privacy Division****

- 5.2 ☐ AND, implement controls and procedures to ensure the CBSA keeps a record documenting whether or not an individual provided consent when it was sought, including a record documenting any withdrawal of consent when applicable.

****Ensure to provide the "controls and procedures" as an annex to this PIA****

- 5.3 ☐ AND, if information is being collected from persons authorized to act on behalf of minors, incompetents or individuals who have been deceased for less than 20 years, implement appropriate mechanisms to ensure that such persons are authorized to act on behalf of individuals who do not have the capacity to provide consent.

****Ensure to provide the "mechanisms" as an annex to this PIA****

NO

- 5.4 ☒

The information collected via PIK is collected directly. While up to five individuals can declare via one kiosk session, each person is required to review and confirm the validity of the information provided.

6. Indirect Collection - Without Notification and Consent

Is personal information collected from another source without notice to or consent from the individual to whom the information relates?

YES

6.1 ☐ Where information is collected indirectly under any of the following circumstances without notice to, or consent from, the individual to whom it relates, please check the applicable boxes and explain as requested:

☐ a) The collection is a result of a disclosure to the CBSA under subsection 8(2) of the *Privacy Act*. State the applicable paragraph(s) of subsection 8(2) and provide a brief explanation for each:

Details: *(This information is mandatory)*

☐ b) Direct notification of the individual might result in the collection of inaccurate information, or might defeat the purpose or prejudice the use for which the information is collected. Briefly explain why notice is not provided: (For example, certain kinds of lawful investigation might be jeopardized if the investigators were required to notify the individuals who were the subjects of the investigations before collecting information indirectly from other sources.)

Details: *(This information is mandatory)*

☐ c) The information involved in the program or activity is to be used solely for a non-administrative purpose in which no decisions are made about the individuals to whom the information relates. (This includes research, statistical, audit or evaluation purposes.)

6.2 ☐ AND, if any of the circumstances in a) b) or c) is applicable, ensure that it is reflected in the relevant **PIB**.

6.3 ☐ AND, if the information is to be used solely for a non-administrative purpose (box c above has been checked), ensure that the requirements under sections 6.3.2 and 6.3.3 of the *Directive on Privacy Impact Assessment* have been met, and that the decision of the official responsible for section 10 of the *Privacy Act* to proceed with a CBSA PIA for the program or activity has been adequately documented in the description of the program or activity in "Section 1 - Overview and PIA Initiation" of the CBSA PIA.

6.4 ☐ OR, if none of the circumstances in a) b) or c) is applicable, then the personal information must be collected directly from the individual, or indirectly with the consent of the individual. Please review the responses to Questions 4 and 5 and ensure that the "**Privacy Notice**" or the "**Consent Statement**" includes all of the required elements within Question 4.

NO

6.5 ☒ All personal information is collected directly from the individual to whom it relates, or from another source with notice to, or consent from, the individual or a person authorized to act on behalf of the individual (see Questions 4 and 5 above).

The information collected via PIK is collected directly. While up to five individuals can declare via one kiosk session, each person is required to review and confirm the validity of the information provided.

7. Retention and Disposal of Personal Information

Has Library and Archives Canada approved a records retention and disposal schedule that applies to the personal information?

YES

- 7.1 ☒ Please identify the Record Disposition Authority (RDA) and describe the retention and disposal schedule:
- 7.2 ☒ AND, implement controls and procedures to ensure that personal information used to make a decision that directly affects an individual will be retained for a minimum of two years after the last administrative action or, where a request for access to the information has been received, until such time as the individual has had the opportunity to exercise all his/her rights under the Act.
- 7.3 ☐ AND, if the CBSA intends to dispose of personal information that has been used for an administrative purpose prior to the expiration of the two-year minimum retention standard established by the *Privacy Regulations*, it must obtain the consent of the individual to whom the information relates before doing so.
- 7.4 ☒ AND, the CBSA must cite the RDA number, the retention period and the disposition standards for the personal information in the relevant **PIB**.

Details: The RDA listed in the PIB is 2000/033, which is an active Records Disposition Authority confirmed through the Library and Archives Records Disposition Authorities Control System. While the terms and conditions list only the Customs Branch of the Canada Customs and Revenue Agency, the authorization portion of the RDA listing includes records collected or held by the CBSA.

The RDA terms and conditions are generic in nature, requesting only that records that are considered to have archival value be transferred to LAC and enable the CBSA to set the required retention period and related destruction for records that are not archival in nature.

The retention standards listed in the Traveller Declaration card PIB reads, "Files are retained for seven years from the date stamped on the traveller's declaration card (date of interview between the traveller and the border services officer or the date stamped on the traveller receipt when the traveller uses the Automated Border Clearance or NEXUS kiosk). After this period, the records are destroyed.

The retention period for information collected via PIK will be aligned with the retention period for the E311 (i.e., seven years).

For the longer term, the CBSA should look into the possibility of internal alignment among CBSA programs or services that collect traveller history information. For example, Traveller Processing and Entry/Exit initiative. Traveller Processing records (entry) are currently held for seven years, consistent with the current Declaration cards retention standard, while retention period for Entry/Exit initiative (exit records) is 15 years past the point of collection.

NO

- 7.5 ☐ Provide a Records Disposition Submission to Library and Archives Canada describing the records containing the personal information for which the institution requires a RDA.

- 7.6 ☐ AND, obtain a RDA from Library and Archives Canada to allow the CBSA, under certain conditions, to dispose of records that no longer have operational utility for the program or activity.
- 7.7 ☐ AND, ensure that all the other applicable requirements listed under "YES" at Question 7 are met.

8. Accuracy of Personal Information

Will measures be adopted to ensure that personal information used by the CBSA for an administrative purpose is as accurate, up-to-date and complete as possible?

YES

- 8.1 Please check any of the following measures that will be adopted to ensure accuracy of the personal information and provide details as requested:
- 8.1.1 ☒ Personal information will be collected directly from the individual to whom it relates or it will be validated with the individual or a person authorized to act on behalf of the individual.
- 8.1.2 ☒ A data-matching process will be used to verify the accuracy of personal information against a "reliable source" (within or outside the CBSA) where this is authorized, or where consent was obtained.
- 8.1.3 ☐ In cases where direct collection or consent is not feasible, the CBSA will obtain information from trusted sources (public or private) and verify accuracy against existing personal information before use.
- 8.1.4 ☒ Technological methods will be used to identify errors and discrepancies.
- 8.1.5 ☐ Other
- 8.2 ☐ AND, if measures are adopted other than "*direct collection or validation with the individual or with a person authorized to act on behalf of the individual*", the CBSA must implement appropriate controls and procedures to ensure that:
- a) the technique(s) and the specific source(s) used to validate or update the personal information are documented;
 - b) individuals are given the opportunity, whenever possible, to request correction of any inaccurate personal information before the information is used in a decision-making process that affects them;
 - c) personal information can only be modified or corrected by those within the CBSA who have the authority to do so;
 - d) when personal information is corrected or annotated, the record of personal information indicates the date of the last correction or annotation and the source of the information used to make the correction or annotation; and
 - d) when personal information is corrected or annotated, other authorized holders of the information are notified about the correction or annotation and that all copies of the information in the possession of the CBSA are corrected / annotated.
- 8.3 ☐ AND, if appropriate, ensure that the "**Privacy Notice**" or "**Consent Statement**" and the relevant **PIB** are amended to identify the data-matching activity including the source(s).

Details: Personal information collected through the PIK will be verified through querying existing CBSA information holdings, such as: Customs Enforcement System (ICES) and Interdiction and Border Alerting System (IBAS). This process includes MRZ, PKD and ePassport chip validation to identify discrepancies. Discrepancies may result in a referral to secondary processing. No information is collected directly through the app, all data is transferred to the kiosk for review and confirmation. PIK will assess the information provided by the traveller and, if discrepancies are noted in CBSA information holding, the individual may be referred to secondary processing. This is an electronic process. Additionally, travellers using the app will be provided with an editable summary of their declaration, for review and confirmation at the kiosk.

NO

8.4 ☐

Explain why such measures will not be adopted: *(This information is mandatory)*

9. Use of Personal Information

Will the personal information collected for the program or activity be used solely for the original purpose for which it was obtained or compiled, a use consistent with that purpose, or a purpose for which the information was disclosed to the institution pursuant to subsection 8(2) of the Privacy Act?

YES

- 9.1 ☒ Implement controls and procedures to ensure that access to the personal information for such purposes will be limited to authorized individuals who need to know the information to perform their official duties.

Details: Internally, access to the information is limited to four directorates: Traveller Transformation; Information, Science and technology; Border Operations; and Recourse. Access to the data systems is defined by user profile.

External to the CBSA, access to the information is limited to other government departments, such as StatCan, who require the information to fulfil their mandate and with whom the CBSA has an established Memorandum of Understanding or information sharing agreement. On an ad-hoc basis, the CBSA receives requests from ESDC and PHAC, to provide declaration information to support program integrity and national health priorities. Access to the data by all parties would be pursuant to *subsection 8(2) of the Privacy Act*. While information sharing agreements and Memorandums of Understanding are in place, they are dated; CBSA is reviewing each agreement to re-confirm the authorities for the collection of information and to ensure only the personal information elements required are being shared.

- 9.2 ☒ AND, ensure that the "Data Flow Diagram" or "Data Flow Tables" completed for "Section 4 – Flow of Personal Information" of the CBSA PIA identify the areas, groups and individuals (e.g., the positions) within the CBSA who have a need-to-know to access to or handle the personal information, including their geographical location and where the personal information will be stored or retained.

- 9.3 ☒ AND, if the purposes for which the personal information is used includes any use(s) of the

information for a non-administrative purpose, (such as research, statistical, audit and evaluation purposes) the CBSA will adhere to the requirements and principles in the **CBSA Privacy Protocol For Non-Administrative Purposes** (2012), in accordance with section 6.2.15 of the *Policy on Privacy Protection*, to address any impact that such non-administrative uses may have on privacy.

NO

- 9.4 ☐ Identify below any other uses of the personal information, in other words, any routine uses that are not directly related to the purpose of the collection, or, which are not consistent with that purpose or for which the information was disclosed to the CBSA pursuant to subsection 8(2) of the *Privacy Act*:

Detail : (This information is mandatory)

- 9.5 ☐ AND, ensure that these other uses are reflected in the relevant **PIB**. (In accordance with subsection 9(1) of the *Privacy Act*, if these other uses are not described in the PIB in CBSA Info Source, the CBSA is required to record each use on the individual's file. Describing them in the PIB is, therefore, a far more efficient practice – see Question 11.)
- 9.6 ☐ AND, include a description of these other uses in the “**Privacy Notice**” or “**Consent Statement**”, as appropriate,
- ☐ AND, ensure the all the other applicable requirements listed under “**YES**” at Question 9 are met.

10. Disclosures Directly Related to the Administration of the Program or Activity

Will personal information be disclosed for purposes directly related to the administration of the program or activity?

YES

- 10.1 ☒ Please check all applicable boxes below and, for each disclosure, identify the name of the organization or third party to which personal information will be disclosed. If it is disclosed within the CBSA, please identify the branch and the program or activity.
- 10.1.1 ☒ Within the CBSA for another program or activity

Details: Within the CBSA, the personal information collected via the PIK will be used in the process of Secondary Processing (traveller processing, whether primary or secondary is considered to be the purpose of the collection). Information is also used internally for enforcement/intelligence, if required. Enforcement / intelligence would relate to the primary purpose of collection and would be considered a consistent use.

- 10.1.2 ☒ Other federal government institutions

Details: Information is disclosed to StatCan as they provide the service of scanning the E311 print Declaration cards. At the same time, StatCan analyses the information providing valuable analytical data back to the CBSA. Aggregate forms of this data may be used by StatCan to inform their statistical travel reports, in support of traveller questionnaires. With PIK, the records will be digital at the point of collection, so StatCan will not be required to scan the E311 cards. They will, however, continue to complete some statistical analysis on the data for the CBSA. As part of the PIK initiative, a review of the

existing information sharing practices and personal information elements required for both traveller processing and statistical analysis was conducted. In doing so, the CBSA validated the data to be shared and has confirmed that only the data elements required by StatCan to carry out their mandate related to travel and tourism will be disclosed. Section 107(5)(b) of the *Customs Act* provides the authority for the disclosure. StatCan does not have a related Personal Information Bank, however, the collection may be represented in the Household Surveys Class of Personal Information.

Information is disclosed to Employment and Social Development Canada (ESDC) – individuals that have been outside the country for more than six days and may be ineligible for residency-based programs (such as Employment Insurance). The data elements collected through PIK to be shared with ESDC and the authorities are being reviewed to ensure only data elements that are required by ESDC to carry out their mandate and for which there is collection/disclosure authority are shared. While the CBSA PIB refers to the ESDC PIB Employment Benefits, Support Measures and Other Programs, consideration should be given to reflecting the ESDC PIB Employment Insurance Program Investigation PIB ESDC PPU 171.

Lastly, in support of health questionnaires, information may be provided to the Public Health Agency of Canada on a case by case basis and upon request so that they may inform travellers who have travelled in close proximity to a potentially contagious individual. Initial assessment information is collected by PHAC in a process external to the PIK collection, however, traveller contact information may be disclosed from the PIK information holdings. The PHAC PIB reference is Traveler Illness Reports, PHAC PPU 071.

10.1.3 ☐ Provincial, territorial or municipal governments institutions

10.1.4 ☒ Foreign government institutions and entities thereof

Details: There are no systematic disclosures to foreign governments however, in the event of criminal activity, enforcement processes may require international collaboration. Any disclosures of personal information for this purpose would be in accordance with the disclosure provisions of section 8(2) of the *Privacy Act*.

10.1.5 ☐ International organizations

10.1.6 ☐ The private sector (e.g., contractor or other external service provider)

10.1.7 ☐ Other

10.2 ☒ AND, ensure that:

- a) any such disclosure is made in compliance with section 8 of the *Privacy Act*, which allows disclosures of personal information with consent of the individual to whom the information relates (subsection 8(1)) or without consent in certain and limited circumstances pursuant to subsection 8(2) of the Act;
- b) only personal information elements that are necessary for the intended purpose are disclosed;
- c) the organization or third party receiving the personal information is authorized to do so;
- d) administrative, physical and technical safeguards appropriate to the sensitivity of the information will be applied to protect the information during and after its transmission (see Question 15);
- e) the organization or third party to which the personal information will be disclosed for the administration of the program or activity are identified in the "Consistent Use" section in the relevant **PIB** in *CBSA Info Source*, including the specific purpose of the disclosure;

the "Privacy Notice" or "Consent Statement" describes any disclosures of information;

- f) the "Data Flow Diagram" or "Data Flow Tables" completed in "Section 4 – Flow of Personal Information" of the CBSA PIA include details on the disclosed personal information:

- 10.3 ☒ AND, any disclosure of personal information to another federal institution or outside the Government of Canada is governed by a formal agreement or arrangement (e.g., a Memorandum of Understanding, an accord, a contractual arrangement, etc.) to ensure that appropriate privacy protection clauses are included, and, where applicable, include provisions for inter-jurisdictional or transborder flows of personal information. Such clauses must cover the following topics:
- a) Control over personal information, where appropriate.
 - b) Limitations on the collection, retention, use and disclosure of personal information.
 - c) Measures (administrative, technical and physical) to protect the integrity and confidentiality of personal information.
 - d) Measures governing the disposition of the personal information, where relevant
 - e) Measures to ensure or verify that the personal information is only used for the purposes related to the agreement, arrangement or contract.
 - f) Obligations are to be extended to other parties such as subcontractors.

Details: Airport Authorities: While there is no disclosure of personal information, a Service Level Agreement will be signed with each airport authority prior to deployment of PIK to provide structure and delineate obligations and control mechanisms, for both the CBSA and the Airport Authority, to ensure the protection of personal information.

Statistics Canada: While a Memorandum of Understanding exists with StatCan, the MoU refers to data collection of E311 declaration, not the collection of information via the PIK process. An Annex to the current MOU is being drafted and will delineate the data elements, process and requirements around the sharing of information with StatCan. Custody, control, retention and disposition will be clearly documented.

NO

- 10.4 ☐ There is no disclosure of personal information within or outside the institution for purposes that are directly related to the administration of the program or activity.

11. Accounting for New Uses or Disclosures Not Reported in CBSA Info Source

Will controls and procedures be implemented to account for any new use or disclosure of the personal information that is not included in the relevant PIB published in CBSA Info Source?

YES

- 11.1 ☒ Appropriate controls and procedures have been or will be implemented to ensure that:
- a) the head of the institution (The ATI and Privacy Director) or the appropriate delegate is notified about any new use or disclosure of personal information that is not reflected in the **PIB** description published in *CBSA Info Source*;
 - b) the consent of the individual to whom the information relates is obtained in writing, as appropriate, prior to any new use of the information for an administrative purpose that is not reflected in the relevant **PIB** published in *CBSA Info Source*, unless the new use is considered to be consistent with the purpose for which the personal information was obtained or compiled and the Privacy Commissioner is notified, by the CBSA ATI and Privacy Director, forthwith regarding the new consistent use;
 - c) except as permitted under subsection 8(2) of the *Privacy Act*, any disclosure of personal information for a purpose that is not reflected in the relevant **PIB** published in *CBSA Info Source* will only be made with the consent of the individual to whom the information relates;
 - d) a record is kept for any new use or disclosure of personal information not described in the relevant **PIB** published in *CBSA Info Source*, and that this record is stored with the personal information to which it relates and retained for a minimum period of two years following such a use or disclosure;
 - e) if the information is disclosed to a federal investigative body under paragraph 8(2)(e) of the *Privacy Act*, the record of disclosure will be kept in a separate PIB for a period of two years where it will be available to the Privacy Commissioner for review upon request;
 - f) the Privacy Commissioner is notified, by the CBSA ATI and Privacy Director, forthwith, as required under subsection 9(4) of the Act, of any new use or disclosure that is consistent with the purpose for which the information was obtained or compiled, but which is not reflected in the relevant **PIB** published in *CBSA Info Source*;
 - g) the relevant **PIB** is amended in time for the next edition of *CBSA Info Source* to include any new use(s) or disclosure(s) that are consistent with the purpose for which the information was obtained or compiled, as well as any routine use(s) or disclosure(s) that do not fall within the categories of purpose of collection or consistent use; and
 - h) the Privacy Commissioner is notified, by the ATI and Privacy Director, prior to or forthwith, as required under subsection 8(5) of the Act, about any disclosures made or to be made in the public interest or in the interest of the individual to whom the information relates.
 - i) Other

NO

- 11.2 ☐ Please explain why such controls and procedures will not be implemented

Detail: *Provide adequate justification.*

12. Safeguards - Statement of Sensitivity

Has a Statement of Sensitivity (SoS) or similar analysis been completed to assess the degree of sensitivity of the personal information to be collected and retained for the program or activity?

YES

- 12.1 ☒ The information contained in the SoS or similar analysis has been taken into account when assessing the level of risks to privacy in "Section 2 - Risk Area Identification and Categorization" of the CBSA PIA.

Details: A Statement of Sensitivity has been prepared for the PIK Initiative and for the eDeclaration mobile application. The information collected by PIK was identified as Protected B, while the information collected via the eDeclaration mobile application was identified as unclassified and non-sensitive.

NO

- 12.2 ☐ Please explain why a SoS or similar analysis was not considered necessary to assess the sensitivity of the information.

13. Safeguards - Threat and Risk Assessment

Has a Threat and Risk Assessment (TRA) or a similar security assessment been completed for the program or activity? (Input to this section must be coordinated with and reviewed by CBSA – IT - Security Directorate)

YES

- 13.1 ☐ Reference the title of the TRA or other security assessment in "Section 6 – Supplementary Documents List" and provide a brief synopsis of the assessment in the space below:

Details :

- 13.2 ☐ AND, obtain assurances from the officials responsible for the program or activity that the measures recommended in the assessment have been implemented to ensure the confidentiality, availability and integrity of the personal information.
- 13.3 ☐ AND, ensure that any residual risks to personal information are known and accepted by the executive or senior official responsible for the program or activity and the Head or delegated authority for the *Privacy Act*. (ATI and Privacy Director)

NO

- 13.4 ☒ If a TRA or similar security assessment is underway, simply reference that fact in the space below and indicate when it is likely to be completed. If there is no intent to complete one, please explain.

Details: The CBSA project processes stipulate Security Assessment Report as the approved Agency project document instead of a Threat and Risk Assessment (TRA). A Preliminary Security Assessment Report (PSAR) has been prepared for the PIK initiative. The Security Assessment Report, as per standard project process, is reviewed and revised as the project progresses and will be finalized just before launch of the PIK initiative in March 2017. As a result, should privacy risks be identified, it may be too late to adequately mitigate the risks before implementation.

The potential risks created by the timing of the SAR in the project process - Service Lifecycle Management Framework (SLMF) - should be raised with the CBSA Management.

14. Safeguards - Administrative, Physical and Technical

Please identify below any administrative, physical and technical safeguards in place, or to be implemented, for this program or activity to ensure the confidentiality, availability and integrity of the personal information.

Please check all that apply, including safeguards identified by the TRA or similar security assessment.

14.1 Administrative safeguards

- ☒ Internal security and privacy policies and procedures
- ☒ Staff training on privacy and the protection of personal information
- ☒ Screening and security checks of employees
- ☒ Appropriate security levels for employees who will have access to personal information
- ☒ Contingency plans and documented procedures in place to identify and respond to security and privacy breaches, and to communicate security violations to the data subject, law enforcement authorities and relevant program managers
- ☒ Regular monitoring of users' security practices
- ☒ Methods to ensure that only authorized personnel who need to know have access to personal information
- ☒ Other

Details: A complete list of administrative safeguards is listed in the R413 System Requirements Specification and will be verified by the R413 Final Security Assessment Report.

14.2 Physical safeguards

- ☒ Restricted access areas
- ☒ Security guards
- ☒ Identification badges are worn by staff at all times
- ☒ After hours alarms and monitoring systems
- ☒ Locked filing cabinets
- ☒ Combination locks
- ☒ Video surveillance (closed-circuit television)
- ☒ Secured server locations
- ☒ Backups secured off-site
- ☒ Other

Details: A complete list of physical safeguards is listed in the R413 System Requirements Specification and will be verified by the R413 Final Security Assessment Report.

14.3 Technical safeguards

- ☒ Role-based user authorization and authentication
- ☒ Passwords (minimum of 6 characters long, include alpha and numeric characters)
- ☒ Passwords are changed by users every 90 days and recently used passwords cannot be re-used)
- ☒ Password protected screensavers
- ☒ Session-time out security (automatically locks an account after a session has been idle for a specified amount of time)
- ☒ Firewalls
- ☒ Virtual Private Network (VPN)
- ☒ Encryption of sensitive information
- ☒ Government of Canada Public Key Infrastructure Certificates (PKI)
- ☒ External Certificate Authority (CA)
- ☒ Audit trails
- ☒ Other

Details: A complete list of technical safeguards is listed in the R413 System Requirements Specification and will be verified by the R413 Final Security Assessment Report.

15. Technology and Privacy - Tracking Technologies

Will the information system(s) used to deliver the program or activity employ cookies or other tracking technologies to collect personal information about users and their transactions?

YES

- 15.1 ☐ The specific tracking technologies to be used is adequately described under Part 6: Technology and Privacy of "Section 2 – Risk Area Identification and Categorization" of the CBSA PIA; (
- 15.2 ☐ AND, the collection of any personal information using such technologies is reflected in the relevant **PIB** and in "Section 3 – Analysis of Personal Information Elements" of the CBSA PIA;
- 15.3 ☐ AND, the use of such technologies to collect information about users and their transactions is adequately reflected in the "**Privacy Notice**";
- 15.4 ☐ AND, those responsible for implementing and using tracking technologies to collect personal information or who may have access to personal information collected through these methods are made aware of privacy and security policy requirements;
- 15.5 ☐ AND, where personal information collected through such tracking technologies is used to make a decision that directly affects the individual to whom the information relates, it will be retained for a minimum of two years after the last administrative action as required under the *Privacy Regulations*.

NO

- 15.6 ☒ Tracking technologies are not used to collect personal information about users.

16. Technology and Privacy - Surveillance or Monitoring

Will the new or modified program or activity result in new or increased surveillance or monitoring of a targeted population?

YES

- 16.1 ☐ Consult with your legal advisors to determine whether or not such surveillance or monitoring activities raise any issues relating to the *Charter of Rights and Freedoms*, the *Privacy Act* or other applicable acts.
- 16.2 ☐ And, ensure the surveillance or monitoring method(s) to be used, the characteristic(s) of the targeted population and the scope of the surveillance or monitoring are adequately described under Part 6: Technology and Privacy of "*Section 2 – Risk Area Identification and Categorization*" of the CBSA PIA.
- 16.3 ☐ AND, any personal information collected or created as a result of such surveillance or monitoring is described in the relevant **PIB** and in *Section 3 – Analysis of Personal Information Elements* of the CBSA PIA.
- 16.4 ☐ AND, the collection or use of personal information through surveillance or monitoring is adequately reflected in the "**Privacy Notice**", unless such notification might result in the collection of inaccurate information or defeat the purpose or prejudice the use for which the personal information is collected.
- ☐ If notice about surveillance or monitoring will not be provided

Detail explain why:

- 16.5 ☐ AND, those responsible for implementing and using such surveillance or monitoring method(s) or who may have access to personal information collected or created through these methods are made aware of privacy and security policy requirements.

NO

- 16.6 ☒ The new or modified program or activity will not result in additional surveillance or monitoring.

17. Considerations Related to Compliance, Regulatory Investigation, Enforcement

Does the program or activity involve compliance/regulatory investigation or law enforcement, surveillance or intelligence gathering that targets specific individuals against whom penalties, criminal charges or sanctions may be applicable?

YES

17.1 ☒ Consult with your legal advisors to determine whether or not the compliance/regulatory investigation or law enforcement activities raise any issues relating to the *Charter of Rights and Freedoms*, the *Privacy Act* or other applicable acts.

17.2 ☒ AND, identify the legislative authority and the specific regulatory or law enforcement purpose involved:

Details: Legal authority for the collection of personal information via traveller processing is derived from multiple, inter-related legislations and regulations.

o Information required for the regulation of goods (import/export) is derived from one legislation and supporting regulations. 1) Section 12 of the *Customs Act*, which states, "all goods that are imported shall, except in such circumstances and subject to such conditions as may be prescribed, be reported at the nearest customs office designated for that purpose that is open for business." And 2) Section 5(3) of the *Reporting of Imported Goods Regulations*, which states, "Goods that are imported by a person arriving in Canada on board a commercial passenger conveyance other than a bus shall be reported in writing."

o Information required from individuals as they request entry into Canada is derived from two legislations. 1) Section 11 of the *Customs Act*, which states, "every person arriving in Canada shall, except in such circumstances and subject to such conditions as may be prescribed, enter Canada only at a customs office designated for that purpose that is open for business and without delay present himself or herself to an officer and answer truthfully any questions asked by the officer in the performance of his or her duties under this or any other Act of Parliament." And 2) Section 18(1) of the *Immigration and Refugee Protection Act* which states, "Every person seeking to enter Canada must appear for an examination to determine whether that person has a right to enter Canada or is or may become authorized to enter and remain in Canada."

In addition to these specific legal authorities, information is also collected under the the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act*, as well as associated regulations made thereunder such as the *Cross-border Currency and Monetary Instruments Reporting Regulations*. Subsection 12(1) of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* states, "every person or entity referred to in subsection (3) shall report to an officer, in accordance with the regulations, the importation or exportation of currency or monetary instruments of a value equal to or greater than the prescribed amount."

Program legislation as defined in the *Customs Act* "means any other Act of Parliament or any instrument made under it, or any part of such an Act or instrument,

(a) that the Governor in Council or Parliament authorizes the Minister, the Agency, the President or an employee of the Agency to administer and enforce, including the *Customs Act*, the *Customs Tariff*, the *Excise Act*, the *Excise Act, 2001*, the *Immigration and Refugee Protection Act* and the *Special Import Measures Act*;

(b) that the Governor in Council or Parliament authorizes the Minister, the Agency, the President or an employee of the Agency to enforce, including the *Agriculture and Agri-Food Administrative Monetary Penalties Act*, the *Canada Agricultural Products Act*, the *Feeds Act*, the *Fertilizers Act*, the *Fish Inspection Act*, the *Health of Animals Act*, the *Meat Inspection Act*, the *Plant Protection Act* and the *Seeds Act*;

(c) under which the Minister or another minister authorizes the Agency, the President or an

employee of the Agency to administer a program or carry out an activity; or

(d) under which duties or taxes collected and paid pursuant to the *Customs Act* are imposed."

- 17.3 ☐ AND, if the legislative authority differs from the legal authority for the program or activity, ensure it is adequately reflected in the response to Question 1 of "Section 5 – Privacy Compliance Analysis" and in "Section 1 – Overview and PIA Initiation" of the CBSA PIA.
- 17.4 ☐ AND, any personal information collected or created as a result of such regulatory or criminal enforcement, surveillance or intelligence gathering program or activity is described in the relevant PIB and in "Section 3 – Analysis of Personal Information Elements" of the CBSA PIA.
- 17.5 ☒ AND, the collection or use of personal information through these compliance / regulatory investigation or enforcement activities is adequately reflected in the "Privacy Notice", unless such notification might result in the collection of inaccurate information or defeat the purpose, or prejudice the use, for which the personal information is collected.

Details: Individuals are notified that the information is collected "for the purposes of administering laws that enforce, prohibit, control or regulate the movement of persons, goods or currency into Canada."

- ☐ If notice about the compliance/regulatory investigation or law enforcement activities will not be provided.

NO

- 17.6 ☐ The program or activity does not involve the conduct of regulatory or criminal enforcement, surveillance or intelligence gathering.

SECTION 6 - Summary of Analysis and Recommendations

This table summarizes the privacy risks identified through the PIA process, and categorizes levels of risk as low, moderate, or high. Risk is defined by factors of impact and likelihood of occurrence. The goal of privacy risk management is to maintain privacy risks within acceptable bounds. The higher ratings provide an indication of priority areas for implementing suggested risk mitigation mechanisms. Criteria for ranking are set as follows:

(L)ow: There is a remote possibility that the risk will materialize and/or the impact of the risk to the program is minor.

(M)oderate: The possibility of the risk materializing is very low although the impact of such a risk is high, *OR* the possibility of the risk materializing is high but the impact of such a risk is minor, *OR* the impact and likelihood of the risk occurring are both determined to be moderate.

(H)igh: There is a near certainty that the risk will materialize if no corrective measures are taken and/or the impact of the risk on the program is severe.

Element	Nature of Risk	L	M	H	Recommendations
---------	----------------	---	---	---	-----------------

Necessity to Collect Personal Information	Currently, there are several PIBs that reflect similar collection of personal information.				Conduct a review of the relevant PIBs and consolidate as appropriate.
Authority for the Collection, Use or Disclosure of the Social Insurance Number	No risks identified.				N/A
Direct Collection - Notification and Consent	No risks identified.				N/A
Indirect Collection - Consent or Authority under Sec. 10 of Privacy Regulations	No risks identified.				N/A
Indirect Collection - Without Notification and Consent	No risks identified.				N/A
Retention and Disposal of Personal Information	CBSA retention period for data collected via traveller processing varies by initiative, from 7 years to 15 years.	X			CBSA to conduct a review of the retention period for information collected via traveller processing, and explore the possibility of aligning the traveller processing records for entry, which are currently retained for seven years, with the retention period for Entry/Exit initiative (exit records), which is set for 15 years retention past the point of collection.
Accuracy of Personal Information	No risks identified.				N/A

With the digital collection of traveller declarations, there is the possibility of limiting the information provided to StatCan to that expressly required as well as providing the information electronically. Accordingly, the current agreement with StatCan needs to be updated to reflect the exact data shared, authorities, and the method of transmission of the information.	X		An Annex to the current MOU with StatCan is being drafted to reflect the exact data to be shared, authorities, and the transmission process of the data.
Information sharing agreements which address the sharing of data with program delivery and health partners are outdated, reflecting legacy collection processes.	X		Information sharing agreements will be reviewed to confirm that the appropriate authorities, data elements and method of transmission are clearly articulated.

Disclosures Directly Related to the Administration of the Program or Activity	No risks identified.				N/A
Accounting for New Uses or Disclosures Not Reported in CBSA Info Source	No risks identified.				N/A
Safeguards - Statement of Sensitivity	No risks identified.				N/A
Safeguards – Threat and Risk Assessment	The Security Assessment Report, as per standard project process, is finalized just before launch of the PIK initiative. As a result, should privacy risks be identified, it may be too late to adequately mitigate the risks before implementation.	L			Raise the potential risks created by the timing of the SAR with the CBSA management responsible for Service Lifecycle Management Framework (SLMF).
Safeguards - Administrative, Physical and Technical	No risks identified.				N/A
Technology and Privacy - Tracking Technologies	No risks identified.				N/A
Technology and Privacy - Surveillance or Monitoring	No risks identified.				N/A
Considerations Related to Compliance, Regulatory Investigation, Enforcement	No risks identified.				N/A

General Privacy Compliance	A PIA has not been conducted for traditional primary inspection by a BSO. As a result, privacy risks of in-person processing for travellers opting not to use PIK are unknown.	L	A PIA be completed for the Generic Passage Flow (GPF) Unified Passage (UPASS) initiative. This initiative will enable a unified operational model with tightly integrated and standardized business processes, information and technology that are used throughout the border processing continuum and includes people, goods, or conveyances in all modes, pre-border, at the border, post border, and applies to all CBSA programs. The project goal is to provide one process and one system for the traveller passage continuum.
----------------------------	--	---	--

SECTION 7 - SUPPLEMENTARY DOCUMENTS LIST

Documents used or related to the CBSA PIA may include:

- Automated Border Clearance Program (ABC) PIA Action Plan, March 2013
- Addendum to the PIA for ABC (formerly EPIL), March 2009
- Correspondence from the OPC, "Privacy Impact Assessment – Automated Border Clearance Program" dated May 11, 2015
- Correspondence from the OPC, "Automated Border Clearance Pilot Project" dated June 23, 2011
- Correspondence from CBSA to the OPC, dated February 22, 2013
- Air Traveller Transformation, Presentation to Corporate Reporting, Audit, Evaluation and Governance, February 12, 2016
- Info Source, Canada Border Services Agency Chapter
- Info Source, Employment and Social Development Chapter
- Info Source, Public Health Agency of Canada Chapter
- Info Source, Statistics Canada chapter
- Information Sharing Agreement with Employment and Social Development Canada
- International Travel Statistics (Memorandum of Understanding between the CBSA and Statistics Canada)
- Modernization of Air Traveller Processing, Backgrounder for the Minister, dated November 2015
- Privacy Impact Assessment, Electronic Primary Inspection Line, September 2008
- Privacy Impact Questionnaire, Primary Inspection Kiosk, dated October 2015
- Service Level Agreement (between CBSA and Airport Authorities for the PIK Solution)
- Statement of Sensitivity for the Primary Inspection Kiosk
- Statement of Sensitivity for CanBorder eDeclaration Mobile Application
- Preliminary Security Risk Assessment
- Security Risk Assessment

SECTION 8 - FORMAL APPROVAL

The following signature represents a commitment to comply with sections 4 to 8 of the *Privacy Act* and the related privacy policy requirements outlined in the CBSA PIA as they relate to the administration of the identified program or activity.



Martin Bolduc, Vice President, Programs Branch

Date

for Feb 22, 2017.

Note: Responsibility for sections 4 to 8 of the *Privacy Act* rests with all employees of government institutions that handle personal information. Officials who manage such programs and activities are responsible for ensuring that such requirements are implemented as part of the administration of the program or activity.

The following signature represents a commitment by the Head of the institution or his/her delegate(s) who is responsible for establishing personal information banks in accordance with section 10 of the *Privacy Act*.



Dan Proulx, Director, Access to Information and Privacy Division

Date

FEB 17 2017

Note: Under the *Privacy Act*, the Head or his/her delegate(s) is responsible for complying with legal and relevant privacy policy requirements related to the approval and registration of personal information banks

Annex A: Privacy Compliance Checklist and Other Considerations

Privacy Compliance Analysis question #	Action required to support legal and policy compliance (cross reference to relevant question of <i>Section 5 – Privacy Compliance Analysis</i>)	Done	To be done
1	Legal authority for the program or activity has been established and is reflected in the relevant PIB.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2	a) The categories and elements of personal information to be collected for the new program or activity have been carefully assessed based, for example, on the CBSA's experience gained with the administration of a similar program or activity. The personal data collected will be limited to only that which is required.)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	b) Categories and elements of personal information have been described in the relevant PIB for the program or activity.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	c) Controls and procedures will be implemented to ensure the CBSA does not collect more personal information than necessary for the program or activity and that a continuing need exists for the personal information and its collection.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
4 and 5	a) All of the requisite "Privacy Notices" and "Consent Statements" that meet the requirements of sections 6.2.9 to 6.2.12 of the <i>Directive on Privacy Practices</i> have been drafted. (Texts of the notices and consent statements must be included as an annex.)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	b) Controls and procedures have been implemented to keep records of individual consents, and to ensure that persons acting on behalf of individuals who do not have the capacity to provide consent have the authority to do so under section 10 of the <i>Privacy Regulations</i> .	<input checked="" type="checkbox"/>	<input type="checkbox"/>
7	a) A Records Disposal Authority (RDA) has been approved by Library and Archives Canada to authorize the disposal of the records containing personal information for the program.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	b) Controls and procedures have been implemented within the program or activity and the CBSA ATI and Privacy Division to ensure that information that has been used for an administrative purpose will be kept for the minimum retention period established by the Privacy Regulations.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	c) Reference to the RDA, the retention period and the disposition standards for the program have been cited in the relevant PIB.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
8	Controls and procedures are in the process of being implemented to ensure that the personal information associated with the program is as accurate, complete and up-to-date as necessary.	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Privacy Compliance
Analysis question #

Action required to support legal and policy compliance
(cross reference to relevant question of *Section 5 – Privacy
Compliance Analysis*)

Done

To be
done

**Other Privacy Considerations related to specific principles that are not explored in the previous 17 sections:
(these considerations should be explored in the Executive Summary)**

Openness

Describe how the results of any privacy impact assessment or audit will be made available to the public. The Executive Summary will be published on the external CBSA ATI and Privacy Division website at <http://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/pia-efvp/atip-aiprp/pias-sefp-eng.html>

☒

☐

Are policies and practices relating to the proposal's management and handling of personal information available to the public?

☒

☐

Is there a communications plan to explain to the public how personal information will be managed and protected?

☒

☐

Is there a clearly defined and easy process for individuals to access such information and/or communicate with appropriate individuals with respect to policies and practices relating to management and protection of personal information?

☒

☐

Where appropriate, will public consultation take place on the privacy implications of the proposal?

☒

☐

Individual's Access
to
Personal Information

Is the system designed to ensure that an individual can have access to his/her personal information, including all other programs or applications that have received copies of the information? s. 12(1)

☒

☐

Are there documented procedures developed or planned on how to make privacy requests or requests for the correction of personal information? s. 12 (2)

☒

☐

Are individuals provided with access to their personal information in the official language of their choice? s. 17(2)

☒

☐

If appropriate, are individuals provided with access to their personal information in an alternative format? s. 17(3)

☒

☐

Challenging
Compliance

Are the complaint procedures for the proposed program or service consistent with legislated requirements? s. 29-35

☒

☐

To improve information management practices and standards, has a procedure been established to log and periodically review the nature, frequency and resolution of complaints?

☒

☐

Primary Inspection Kiosk

PIA

Privacy Compliance Analysis question #	Action required to support legal and policy compliance (cross reference to relevant question of <i>Section 5 – Privacy Compliance Analysis</i>)	Done	To be done
	Are there oversight and review mechanisms implemented or available to ensure accountability?	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Have oversight agencies, including the Office of the Privacy Commissioner, issued reports or opinions on issues that would be relevant to the proposal?	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Annex B

Privacy Statement – Primary Inspection Kiosk

The information that you are providing at the Primary Inspection Kiosk is collected under the authority of Section 12 of the *Customs Act*, Subsection 5(3), Reporting of Imported Goods Regulations, the Customs Tariff, the *Immigration and Refugee Protection Act* and/or the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* for the purposes of administering laws that enforce, prohibit, control or regulate the movement of persons, goods or currency into Canada. This includes facilitating compliance with reporting obligations under this legislation and the collection of duties and taxes owing on goods imported into Canada.

Failure to provide/complete all the requested information will result in your referral to a Border Services Officer for in-person processing.

This information may be used in support of ongoing CBSA investigation or enforcement activities. This information may also be disclosed to:

- Other government departments and agencies, police forces and other countries to administer laws that prohibit, control and regulate the importations of goods;
- Other government departments, such as Statistics Canada, the Public Health Agency of Canada, and Employment and Social Development Canada and for the purpose of statistical reporting public health and program integrity.

Your photograph will be taken for the purposes of administration and/or enforcement of the *Customs Act* or *Immigration and Refugee Protection Act* and may also be used for the administration or enforcement of other legislation or regulations administered or enforced by the CBSA. It will also be retained in accordance with the *Privacy Act*.

Individuals have the right of access to and/or can request corrections of their personal information under the *Privacy Act*. The information is described within Info Source, Traveller Declaration cards Personal Information Bank CBSA PPU 018 at <http://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/pia-efvp/atip-aiprp/infosource-eng.html>. Should you have concerns about the CBSA's handling of your personal information you have a right to file a complaint with the Privacy Commissioner of Canada.

Annex C

Privacy Statement – CanBorder eDeclaration Mobile App

The CanBorder e-Declaration mobile application is designed to ensure your privacy and protect your personal information. This stand-alone application collects and stores only basic, non-sensitive information, to facilitate your arrival. When you scan your QR code at a Primary Inspection Kiosk in Canada, your information is transmitted securely to the CBSA. CBSA reconciles your eDeclaration with your legal name when you scan your travel document at the kiosk. After 24 hours, your QR code will automatically expire and all declaration data will be purged from the app. You can also manually delete all application data at any time.

The information you are providing at the Primary Inspection Kiosk is collected under the authority of Section 12 of the *Customs Act*, Subsection 5(3), Reporting of Imported Goods Regulations, the Customs Tariff, the *Immigration and Refugee Protection Act* and/or the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* for the purposes of administering laws that enforce, prohibit, control or regulate the movement of persons, goods or currency into Canada. This includes facilitating compliance with reporting obligations under this legislation and the collection of duties and taxes owing on goods imported into Canada.

Failure to provide/complete all the requested information will result in your referral to a Border Services Officer for in-person processing.

This information may be used in support of ongoing CBSA investigation or enforcement activities. This information may also be disclosed to:

- Other government departments and agencies, police forces and other countries to administer laws that prohibit, control and regulate the importations of goods;
- Other government departments, such as Statistics Canada, the Public Health Agency of Canada, and Employment and Social Development Canada and for the purpose of statistical reporting public health and program integrity.

Your photograph will be taken for the purposes of administration and/or enforcement of the *Customs Act* or *Immigration and Refugee Protection Act* and may also be used for the administration or enforcement of other legislation or regulations administered or enforced by the CBSA. It will also be retained in accordance with the *Privacy Act*.

Individuals have the right of access to and/or can request corrections of their personal information under the *Privacy Act*. The information is described within Info Source, Traveller Declaration cards Personal Information Bank CBSA PPU 018 at <http://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/pia-efvp/atip-aiprp/infosource-eng.html>. Should you have concerns about the CBSA's handling of your personal information you have a right to file a complaint with the Privacy Commissioner of Canada.



Temporary Foreign Worker Program

Information Sharing Agreement Between the Canada Border Services Agency and Employment and Social Development Canada

Privacy Impact Assessment

TFWP
September 25, 2015/Version 11

The word "Canada" is written in a white, serif font on a dark background. To the left of the text is a stylized graphic of a maple leaf, composed of several overlapping, curved shapes that form the leaf's outline.

Canada

Version Control

Version	Author	Action	Date
0.1	Greg Thompson	Initial Draft	January 28, 2015
0.2	Greg Thompson	Edits from Subject Matter Experts	March 31, 2015
0.3	Vanessa Malik	Edits from Subject Matter Experts	April 10, 2015
0.4	Vanessa Malik	Edits from Subject Matter Experts	May 5, 2015
0.5	Vanessa Malik	Edits from Subject Matter Experts	May 6, 2015
0.6	Vanessa Malik	Edits from Subject Matter Experts	July 27, 2015
0.7	Vanessa Malik	Edits from Subject Matter Experts	July 31, 2015
0.8	Vanessa Malik	Final edits from ATIP Division	August 12, 2015
0.9	Vanessa Malik	Final edits from EIPD	August 24, 2015
10	Vanessa Malik	Final review	September 1, 2015
11	Vanessa Malik	DG changes – for final approval	September 25, 2015

Table of Contents

VERSION CONTROL	2
EXECUTIVE SUMMARY	5
ABBREVIATIONS AND ACRONYMS	10
DEFINITIONS	12
INTRODUCTION	13
SECTION 1 - OVERVIEW AND INITIATION	24
SECTION 2 - RISK AREA IDENTIFICATION AND CATEGORIZATION	30
Type of Program or Activity	30
Type of Personal Information Involved and Context	31
Program or Activity Partners and Private Sector Involvement	31
Duration of the Program or Activity	32
Program Population	32
Technology and Privacy	32
Personal Information Transmission	33
Risk Impact to the CBSA	34
Risk Impact to the Individual or Employee	34
SECTION 3 - ANALYSIS OF PERSONAL INFORMATION ELEMENTS	35
SECTION 4 - FLOW OF PERSONAL INFORMATION	65
4.1 Data Flow Model - Diagram	65
4.2 Determine Eligibility and Admissibility of FW at POE	66
4.3 Request and Receive Tip Line Information (ESDC Disclosure to CBSA)	72
4.4 Receipt of Information After an Employer Compliance Review and/or Inspection	76
4.5 Public Interest Disclosure	76
4.6 Data Flow Model - Table	77
4.7 Internal Use and Disclosure	77
4.8 External Use and Disclosure	78
4.9 Retention / Storage	78
4.10 Other Possible Considerations	79
SECTION 5 - PRIVACY COMPLIANCE ANALYSIS	81
1. Legal Authority For Collection Of Personal Information (if unsure, consult with Legal Services)	81
2. Necessity To Collect Personal Information	82
3. Authority For the Collection, Use or Disclosure Of the Social Insurance Number ...	82
4. Direct Collection - Notification and Consent (as appropriate)	83
5. Indirect Collection - Consent or Authority Under Sec. 10 of Privacy Regulations ...	85
6. Indirect Collection - Without Notification and Consent	85
7. Retention and Disposal of Personal Information	87
8. Accuracy Of Personal Information	87
9. Use Of Personal Information	89
10. Disclosures Directly Related to the Administration of the Program or Activity	90
11. Accounting For New Uses or Disclosures Not Reported in CBSA Info Source	92
12. Safeguards - Statement Of Sensitivity	93

13. Safeguards - Threat and Risk Assessment	94
14. Safeguards - Administrative, Physical and Technical.....	95
15. Technology and Privacy - Tracking Technologies	96
16. Technology and Privacy - Surveillance or Monitoring	97
17. Considerations Related to Compliance, Regulatory Investigation, Enforcement ..	98
SECTION 6 - SUMMARY OF ANALYSIS AND RECOMMENDATIONS.....	99
SECTION 7 - SUPPLEMENTARY DOCUMENTS LIST	109
SECTION 8 - FORMAL APPROVAL	110
ANNEX A: PRIVACY COMPLIANCE CHECKLIST AND OTHER CONSIDERATIONS.....	111
ANNEX B: OFFICE OF THE PRIVACY COMMISSIONER EXPECTATIONS	114
ANNEX C: CATEGORIES OF PERSONAL INFORMATION	117
ANNEX D: LABOUR MARKET IMPACT ANALYSIS APPLICATION.....	119
ANNEX E: APPOINTMENT OF A 3 RD PARTY REPRESENTATIVE (FOR LMIA APPLICATION)	
.....	133
ANNEX F: WORK PERMIT APPLICATION (FORM IMM 1295).....	136
ANNEX G: TEMPORARY RESIDENT VISA APPLICATION (FORM IMM 5257)	140
ANNEX H: ESDC'S ONLINE FRAUD REPORTING TOOL	142
ANNEX I: CBSA LEAD REFERRAL FORM (FROM ESDC INTEGRITY SERVICES BRANCH)...	144
ANNEX J: INFORMATION SHARING AGREEMENT BETWEEN ESDC AND THE CBSA	146

LIST OF TABLES

Table 1: Examples of When WPs, Visas, and/or LMIAs are Required.....	14
Table 2: Method of Delivery for Information Exchange	19
Table 3: Personal Information Disclosed by ESDC to the CBSA	35
Table 4: Criminal Charges/Conviction Information Disclosed by the CBSA to ESDC	63

LIST OF FIGURES

Figure 1: Delivery Method for Information Exchange Between ESDC and the CBSA.....	20
Figure 2: Determine Eligibility and Admissibility of Foreign National for TFWP	70
Figure 3: Determine Eligibility and Admissibility of Foreign National at POE for TFWP .	71
Figure 4: Request and Receive Tip Line Information (ESDC Disclosure to CBSA CID).....	75

Privacy Impact Assessment Date / Version:	YYYY-MM-DD (Date sent to OPC)/Version: 10
Office of the Privacy Commissioner file #:	Unassigned
ISA Effective Date	2015-04-16
Federal Institution:	Canada Border Services Agency (CBSA)
Related Class of Record Number:	CBSA ADM 135
Personal Information Bank:	CBSA PPU 050
Government Official Responsible for PIA:	Peter Hill, A/Vice President, Programs Branch
Delegate for section 10 of the <i>Privacy Act</i> :	Dan Proulx, ATIP Director

EXECUTIVE SUMMARY

The Temporary Foreign Worker Program (TFWP), governed by the *Immigration and Refugee Protection Act* (IRPA) and the *Immigration and Refugee Protection Regulations* (IRPR), is jointly administered by Citizenship and Immigration Canada (CIC), Employment and Social Development Canada (ESDC) and the Canada Border Services Agency (CBSA). The TFWP allows Canadian employers to hire foreign nationals (FNs) to fill temporary labour and skill shortages when qualified Canadian citizens or permanent residents are unavailable.

On June 20, 2014, the Ministers of ESDC, and CIC announced comprehensive reforms to the TFWP, including the splitting of the TFWP into the following two programs:

1. TFWP - includes all streams of work for which a Labour Market Impact Assessment (LMIA) is required; and
2. International Mobility Program (IMP) – includes all streams of work that are LMIA-exempt under the *IRPR*.

The Ministers also committed to improving TFW information sharing among federal departments and with provinces and territories.

For employers who have been unable to recruit Canadian citizens or permanent residents for available jobs, the TFWP makes it possible to hire workers from abroad or qualified temporary foreign workers (TFWs) already in Canada.

While most TFWs will be hired to address a specific, short-term labour need, some TFWs who initially came to fill a temporary vacancy can transition to permanent residence if they meet certain requirements. These routes exist to ensure that workers who have shown that their skills are in continuing demand and that they have already adapted well to life in Canada can build a future here.

The documents required for a FN to work legally in Canada vary based on the citizenship of the FN and the nature of the work to be performed in Canada. The documents required may include one or all of the following:

1. Labour Market Impact Assessment

An LMIA is a labour market verification process whereby ESDC assesses an offer of employment to ensure that the employment of a FN will not have a negative impact on the Canadian labour market. A positive LMIA from ESDC is generally required to support a work permit (WP) application, unless CIC deems the position LMIA-exempt, which depends on the occupation and specific case circumstances. In 2013, approximately 38% of TFWs (176,613 individuals) required an LMIA, whereas 62% (284,050) were LMIA-exempt. When an LMIA is required, an LMIA application (See Annex D) is submitted by the employer to ESDC. Employers may also submit a form authorizing a 3rd party representative to engage with ESDC/Service Canada for the purpose of the LMIA application (See Annex E). ESDC reviews the employer's application, ensures TFWP requirements are met, and assesses the likely impact of the TFW(s) on Canada's labour market. ESDC issues a positive LMIA (also known as an ESDC Confirmation) when the employment of the FN(s) is not expected to have a negative impact on Canada's labour market.

2. Visa

In addition to a WP, some prospective TFWs require a visa, which authorizes travel from the foreign country to Canada. Visas are an official counterfoil document, issued by a CIC visa office abroad which is placed in the FNs passport to show that he or she has met the requirements for travel to Canada as a temporary resident (a visitor, student or worker). Citizens of certain countries and territories require a visa to travel to Canada (e.g. Brazil), whereas citizens of other countries do not (e.g. United States of America).

3. Work Permit

In general, all FNs coming to work in Canada require a WP, unless otherwise exempted under section 186 of the IRPR. WP applications for visa-required FNs are submitted to CIC at a visa office abroad. If the WP application is approved, a "Letter of Introduction" is provided by CIC to the FN for presentation to the CBSA at the Port of Entry (POE). Visa-exempt FNs may apply for a WP directly at the POE upon arrival in Canada. In these cases, the WP assessment is completed by the CBSA Border Services Officer (BSO). It is noted that CIC does not issue WPs abroad. The official WP document is only issued by the CBSA at the POE, if the necessary admissibility and eligibility criteria have been met. CBSA officers at POE make the final decision as to who may enter and work in Canada.

In addition to the TFWP, the Federal Skilled Worker Program (FSWP) promotes the immigration of skilled workers to Canada. Under the FSWP, ESDC is required to provide an LMIA for the position being offered to the skilled worker.

Roles of Each Government Institution

The TFWP and the FSWP are jointly administered by ESDC, CIC and the CBSA.

When an LMIA is required, ESDC reviews the employer's application, ensures appropriate program requirements are met, and assesses the likely impact of the employment of the FNs on Canada's labour market. Information collected and used to develop an LMIA includes: employer business and personal information, personal information about the prospective foreign workers, and employer compliance information, including Employer Compliance Review (ECR) and Employer Inspection results (if applicable).

CIC reviews visa and WP applications (primarily from visa-required FNs), issues visas and authorizes WPs when required. CIC is also responsible for the administration of the IMP. The IMP includes the occupations and streams of work for which an LMIA is not required, and its primary objective is to advance Canada's broad economic and cultural interest.

The CBSA performs an important role in the administration and enforcement of the TFWP, FSWP and the IMP by determining the admissibility of prospective foreign workers, issuing WPs at POEs, investigating and removing FNs who work illegally or are otherwise in Canada without status and investigating and prosecuting alleged offences under the IRPA.

Current and Future Information Sharing

Historically, the CBSA and ESDC have exchanged information on companies and individuals to support the CBSA's mandate to enforce IRPA/IRPR and ESDC's role in providing an opinion on the impact that the employment of FNs is likely to have on Canada's labour market, but this exchange has been in limited circumstances and only when it meets the criteria of s. 34(1) of ESDC's legislation, the *Department of Employment and Social Development Act* (DESDA). Conversely, the CBSA has provided information to ESDC on individuals and companies who are being prosecuted or have been convicted of criminal offences related to IRPA/IRPR; this information is used by ESDC to assist in processing current and future applications in the TFWP and FSWP.

In Economic Action Plan 2013, the Government of Canada committed to reforming the TFWP to protect foreign workers from abuse and exploitation, and to reinforce the principle that Canadians should be considered first for available jobs. The 2014 Budget committed significant funding for ESDC to make changes to the LMIA process and introduce reforms relating to LMIA-exempt situations. The reforms to the TFWP are aimed at:

- Reducing employer use and reliance on TFWs;
- Ensuring that employers who abuse the Program face significant consequences;
- Restricting access to the Program; and
- Improving labour market information.

As part of these initiatives, ESDC will invest more time and money into identifying and deterring employer non-compliance with TFWP conditions. In addition, both CIC and ESDC intend to increase their inspection activities and to seek authority to compel documents from third parties that establish employer non-compliance. As a result, CBSA referrals for criminal investigations are expected to increase.

To facilitate the information sharing, the two departments agreed to work together to amend the *Department of Employment and Social Development Regulations* (DESDR) to recognize the CBSA as a prescribed federal institution for the purposes of section 35 of DESDA (i.e. a law enforcement body recognized in the Act), which would allow ESDC to disclose information collected under the TFWP and FSWP to the CBSA for the administration and enforcement of the IRPA.

Further to those legislative/regulatory changes, an Information Sharing Agreement (ISA) was signed between the CBSA and ESDC to enumerate the personal information which will be exchanged between the two departments. The ISA is attached to this PIA as Annex J.

As reflected in the ISA, data will be exchanged between the two institutions in one of three modes. First,

so that BSOs can view LMIA data when the prospective TFW seeks entry to Canada. will be established and maintained by ESDC for both institutions to share information pursuant to the ISA. will be available for a short period of time before it is removed (currently set at records And lastly, in some cases, paper

The personal information disclosed by ESDC to the CBSA will support the administration and enforcement of the IRPA/IRPR and will be limited to information collected on the LMIA application forms, other information related to the LMIA process, information received by ESDC via the TFWP's Online Fraud Reporting Tool, and Service Canada's Confidential Tip Line. Annexes C and D of the ISA stipulate the data elements which ESDC may disclose to the CBSA.

The CBSA will provide information to ESDC regarding anyone who has submitted an application under the TFWP/FSWP and against whom charges have been laid as well as any convictions that may have been rendered. Annex E of the ISA stipulates the data elements which the CBSA may disclose to ESDC.

Privacy Risks Identified in the Development of this PIA

In assessing the ISA, the legislative changes, and work flows that support data exchanges between the CBSA and ESDC, the following privacy risks and corresponding mitigation activities were identified.

Risk #	Risk Description	Mitigation Activity
1	There is a risk that personal information could be disclosed to/by the CBSA and used for a purpose that is beyond the scope of the ISA. Furthermore, there is a risk that CBSA staff may be unaware of the limitations of the ISA and that an offence provision within DESDA may apply to them and the CBSA if they disclose information received from ESDC in contravention to the ISA/DESDA.	All relevant staff will be made aware of the parameters of the ISA and that disclosures to/by the CBSA must be limited to those authorized under the current ISA. Operational guidance will be developed and provided to staff that outlines the limitations of the ISA, as well as the applicable offence provisions within DESDA. In addition, measures to appropriately identify ESDC information held within CBSA systems will be introduced.
2	There is a risk that information obtained from ESDC pursuant to the ISA may be disclosed to a third party in contravention of the disclosure clauses of the ISA. Currently, information received from ESDC may not be appropriately identified/marked as originating from ESDC, and subject to the unique disclosure restrictions of the DESDA.	The CBSA will implement procedures to clearly identify ESDC records that are shared pursuant to the ISA. This will apply to both paper records and data that are stored in CBSA systems. Furthermore, BSOs will be made aware that restrictions to the sharing of ESDC information also apply to information obtained via the FWS-FOSS/FWS-GCMS one way interface.
3		
4	The current disclosure of information by ESDC	This risk has been addressed. Protected B

Risk #	Risk Description	Mitigation Activity
	<p>to the CBSA via the Online Fraud Reporting Tool</p> <p>When ESDC staff complete the CBSA Lead Referral Form, it may be sent to CBSA (Criminal Investigations Division)</p>	
5	<p>When information is needed by the CBSA to support legal proceedings (i.e. prosecution), a request is sent to ESDC's TFWP</p> <p>However, there may be instances where with investigative details designated as Protected B information are sent to ESDC</p>	<p>The CBSA and ESDC will make every reasonable effort to ensure that the transmission of information</p>

ABBREVIATIONS AND ACRONYMS

The following is a list of abbreviations and acronyms used in this report:

AEO	Arranged Employment Opinion
ATIP	Access to Information and Privacy
BSO	Border Services Officer
CAIPS	Computer-Assisted Immigration Processing System
CBSA	Canada Border Services Agency
CIP	Criminal Investigations Program
CIIMS	Criminal Investigations Information Management System
COB	Country of Birth
COR	Class of Record
DESDA	<i>Department of Employment and Social Development Act</i>
DOB	Date of Birth
DSO	Departmental Security Officer
ECR	Employer Compliance Review
EIOD	Enforcement and Intelligence Operations Directorate
ESDC	Employment and Social Development Canada
FN	Foreign National
FOSS	Field Operational Support System
FTP	File Transfer Protocol
FSWP	Federal Skilled Worker Program
FWS	Foreign Worker System
GCMS	Global Case Management System
GC	Government of Canada
HQ	Headquarters
ICES	Integrated Customs Enforcement System
IEOD	Inland Enforcement Operations Division
IMP	International Mobility Program
IMS	Intelligence Management System
IA	Intelligence Analyst
IO	Intelligence Officer

IOAD	Intelligence Operations and Analysis Division
ISA	Information Sharing Agreement
ISB	Integrity Services Branch (within ESDC)
IT/IM	Information Technology/Information Management
LMIA	Labour Market Impact Assessment
LMO	Labour Market Opinion
LOU	Letter of Understanding
MOU	Memorandum of Understanding
NAFTA	North American Free Trade Agreement
NCMS	National Case Management System
OFRT	Online Fraud Reporting Tool
OPC	Office of the Privacy Commissioner of Canada
PA	<i>Privacy Act</i>
PGS	Policy on Government Security
POC	Privacy Oversight Committee
PPSC	Public Prosecution Service of Canada
PIA	Privacy Impact Assessment
PIB	Personal Information Bank
POE	Port of Entry
PR	Permanent Resident
SA&A	Security Assessment and Authorization
TBS	Treasury Board Secretariat
TFW	Temporary Foreign Worker
TFWP	Temporary Foreign Worker Program
TR	Temporary Resident
TRA	Threat and Risk Assessment
TRV	Temporary Resident Visa
VP	Vice-President
VPN	Virtual Private Network
WCA	Written Collaborative Agreement
WP	Work Permit

DEFINITIONS

This section provides definitions of the terms frequently used in this report:

Action Plan	The Action Plan describes the steps that the Program will take to address risks that have been identified by ATIP Division, OPC and TBS.
Administrative purpose	The <i>Privacy Act</i> defines an "administrative purpose" to be the use of an individual's personal information in a decision-making process that directly affects that individual.
Confidentiality	The Government Security Policy (2002) defines "confidentiality" to be the attribute that mandates that the information concerned must not be disclosed to unauthorized individuals, because of the resulting injury to national or other interests, and more specifically, because such disclosure would be contrary to provisions of the <i>Access to Information Act</i> and the <i>Privacy Act</i> .
Consistent use	A use that has a reasonable and direct connection to the original purpose(s) for which the information was obtained or compiled. This means that the original purpose and the proposed purpose are so closely related that the individual would expect that the information would be used for the consistent purpose, even if the use is not spelled out.
Data Matching	A comparison of personal data obtained from a variety of sources, including personal information banks, for the purpose of making decisions about the individuals to whom the data pertains. Data matching is a specialized activity involving the collection, use and disclosure of personal information that is subject to the various requirements of the <i>Privacy Act</i> .
Info Source	Is a series of annual Treasury Board Secretariat publications in which government institutions are required to describe their institutions, program responsibilities and information holdings, including PIBs and classes of personal information. The descriptions are to contain sufficient clarity and detail to facilitate the exercise of the right of access under the <i>Privacy Act</i> . Data-matching activities, use of the SIN and all activities for which privacy impact assessments were conducted have to be cited in <i>Info Source</i> PIBs, as applicable. The <i>Info Source</i> publications also provide contact information for government institutions as well as summaries of court cases and statistics on access requests.
Personal Information	Personal Information: Information about an identifiable individual as defined in section 3 of the <i>Privacy Act</i> . This definition, although lengthy, is not exhaustive, as indicated by the introductory phrase, "including, without restricting the generality of the foregoing". Information that is not specifically mentioned in the list may still be included in the definition of personal information if it qualifies as "information about an identifiable individual".
Personal Information Bank	Is a description of personal information that is organized and retrievable by a person's name or by an identifying number, symbol or other particular assigned only to that person. The personal information described in the personal information bank has been used, is being used, or is available for an administrative purpose and is under the control of a government institution.
Privacy	The Office of the Privacy Commissioner of Canada describes "privacy" as "... the right to control access to one's person and information about one's self. The right to privacy means that individuals get to decide what and how much information to give up, to whom it is given, and for what uses."

INTRODUCTION

The Temporary Foreign Worker Program (TFWP) is governed by the *Immigration and Refugee Protection Act* (IRPA) and the *Immigration and Refugee Protection Regulations* (IRPR), and is jointly administered by Citizenship and Immigration Canada (CIC), Employment and Social Development Canada (ESDC) and the Canada Border Services Agency (CBSA). The Program enables employers in Canada to bring over 300,000 temporary foreign workers (TFWs) to Canada every year to meet their short-term skill and labour needs when Canadian citizens or permanent residents are unavailable.

For employers who have been unable to recruit Canadian citizens or permanent residents for available jobs, the TFWP makes it possible to hire workers from abroad or qualified foreign workers already in Canada.

While most TFWs will be hired to address a specific, short-term labour need, some TFWs who initially came to fill a temporary vacancy can transition to permanent residence if they meet certain requirements. These routes exist to ensure that workers who have shown that their skills are in continuing demand and that they have already adapted well to life in Canada can build a future here.

A. Overview of the Program

The following requirements may apply to an applicant under the TFWP, depending on the particular circumstances of the case:

1. Labour Market Impact Assessment

An employer usually must request a Labour Market Impact Assessment (LMIA), issued by ESDC, before hiring a foreign worker.

A positive LMIA from ESDC is generally required to support a work permit (WP) application, unless CIC deems the position to be LMIA-exempt, which depends on the occupation and case specific circumstances. In 2013, approximately 38% of TFWs (176,613 individuals) required an LMIA; whereas 62% (284,050) were LMIA-exempt. When an LMIA is required, an LMIA application (See Annex D) is submitted by the employer to ESDC. Employers may also submit a form authorizing a 3rd party representative to engage with ESDC/Service Canada for the purpose of the LMIA application (See Annex E). ESDC reviews the employer's application, ensures TFWP requirements are met, and assesses the likely impact of the TFW(s) on Canada's labour market. ESDC issues a positive LMIA (also known as an ESDC Confirmation) when the employment of the foreign nationals (FNs) is not expected to have a negative impact on Canada's labour market.

2. Visa

Some prospective TFWs require a visa, which authorizes travel from the foreign country to Canada. Visas are an official counterfoil document, issued by a CIC visa office abroad which is placed in a FN's passport to show that he or she has met the requirements for travel to Canada as a temporary resident (a visitor, student or worker). Citizens of certain countries and territories require a visa to travel to Canada (e.g. Brazil), whereas citizens of other countries do not (e.g. United States of America).

3. Work Permit

A WP is a document that authorizes a person to work legally in Canada. It sets out conditions for the worker such as:

- the type of work they can do;
- the employer they can work for;
- where they can work; and
- how long they can work.

In general, all FNs coming to work in Canada require a WP, unless otherwise exempted under section 186 of the IRPR. WP applications for visa-required FNs are submitted to CIC at a visa office abroad. If the WP application is approved, a “Letter of Introduction” is provided by CIC to the FN for presentation to the CBSA at the POE. Visa-exempt FNs may apply for a WP directly at the POE upon arrival in Canada. In these cases, the WP assessment is completed by the CBSA Border Services Officer (BSO). It is noted that CIC does not issue WPs abroad. The official WP document is only issued by the CBSA at the POE, if the necessary admissibility and eligibility criteria have been met. CBSA officers at POE make the final decision as to who may enter and work in Canada.

Depending on the circumstances of the employer and the FN, a WP, visa, and/or LMIA may be required. Table 1 provides a few examples of when one, two, or all three may be required.

Table 1: Examples of When WPs, Visas, and/or LMIAs are Required

Scenario	WP	Visa	LMIA
An American professional hockey player, playing for a team in the United States, travels to Montreal for a game.	Not Required	Not Required	Not Required
A Colombian playing basketball for an American university travels to Canada for an exhibition game.	Not Required	Required	Not Required
An American travels to Canada to perform emergency repairs on commercial/industrial equipment that, while unrepared, is disrupting employment of Canadians.	Required	Not Required	Not Required
A Brazilian nanny being hired by a family residing in Canada.	Required	Required	Required

B. Federal Skilled Worker Program (assessed under section 82 and section 203 of IRPR)

On May 4, 2013 the LMIA replaced the former Arranged Employment Opinion (AEO) that was provided by Service Canada to employers who have made an offer of permanent employment to a skilled temporary foreign worker (TFW) in support of their application for permanent residence. Under the FSWP, ESDC and Service Canada are mandated to provide an opinion on an employer’s permanent, full-time job offer to a TFW. If a positive LMIA is issued, the foreign national may receive 10 points to support their permanent residence application for having “arranged employment” in Canada.

Under the FSWP, the definition of “arranged employment” has not changed and means an offer of employment in an occupation listed in Skill Type O Management Occupations or Skill Level A or B of the *National Occupational Classification* matrix. Refer to R182 of IRPR for more details.

C. Roles and Responsibilities

The TFWP and the FSWP are jointly administered by ESDC, CIC and the CBSA. The specific roles of each organization are detailed below.

1. ESDC

ESDC is mandated under the IRPA to provide an assessment of the potential labour market impact of the entry of TFWs into Canada’s workforce, in the form of the LMIA; formerly called a Labour Market Opinion (LMO). Information collected and used to develop an LMIA includes: employer business and personal information, personal information about the prospective foreign workers, and employer compliance information, including Employer Compliance Review (ECR) and Employer Inspection results (if applicable). When an LMIA is required, ESDC reviews the employer’s application, ensures appropriate program requirements are met, and assesses the likely impact of the employment of the FNs on Canada’s labour market.

As reflected in the Privacy Notice Statement on an LMIA, the information provided by employers on an LMIA application may be shared with CIC for the administration and enforcement of the IRPA and IRPR as permitted by the *Department of Employment and Social Development Act* (DESDA)², and may be accessed by the CBSA for the purpose of issuing WPs at POEs. ESDC may also provide information to CBSA in order for that agency to investigate and enforce the IRPA and IRPR in relation to an LMIA.

ESDC also performs ECRs and employer inspections to ensure compliance with program requirements.

2. CIC

CIC is responsible for reviewing and processing visas and WPs, and issues visas and authorizes WPs when required. Following receipt of a WP application including a copy of the ESDC confirmation letter that confirms the employer received a positive LMIA (when required), a CIC visa office abroad reviews the application and, after assessing both program and admissibility requirements, either approves or refuses the WP application. If the WP application is approved, CIC will issue a “Letter of Introduction” to the FN.

Also, CIC administers the International Mobility Programs (IMP), which allows particular TFWs to be LMIA-exempt. For example, labour mobility is a key part of the North American Free Trade Agreement (NAFTA). NAFTA provides reciprocal benefits, allowing FNs in certain occupations from partner countries to work in Canada without the requirement to obtain an LMIA, as well as allowing Canadians to work abroad with similar privileges. While about 12,000 Americans worked in Canada through the NAFTA professional occupation provision in 2011, the number of Canadians working in the United States through the same provision more than tripled that, with about 39,000 in all.

By exempting some FNs from needing an LMIA before being able to work in Canada, the IMP aims to provide competitive advantages to Canada and reciprocal benefits to Canadians.

² Formerly called the *Human Resources and Skills Development Act* (HRSDA).

As part of its responsibilities to administer the TFWP and the IMP, CIC is also responsible for inspections of IMP employers. This authority was introduced in 2013 via amendments to the IRPA/IRPR. To date, however, CIC has not undertaken any inspection activities under the new authority. CIC will be entering into an arrangement with Service Canada so that Service Canada's Integrity Services Branch will perform certain IMP inspections on behalf of CIC.

3. CBSA

The CBSA is responsible for the administration and enforcement of the TFWP and the FSWP at Canadian POEs and inland.

CBSA officers at POE determine the admissibility of FNs to Canada, assess WP applications (for visa-exempt FNs), verify the eligibility of prospective foreign workers, and issue WPs, if the necessary criteria are met. When a WP is issued, the BSO will explain any associated conditions. For WP applications that are assessed by CIC at a visa office abroad, if CIC approves the WP application a "Letter of Introduction" is issued. However, the final determination of a FN's admissibility to Canada can only be made by a BSO at the time the FN seeks entry into Canada. The decision to issue a WP to any FN rests with the BSO in accordance with the requirements of the IRPA and IRPR. As such, FNs seeking entry to work in Canada are not guaranteed a WP, even if CIC issues the "Letter of Introduction".

CBSA inland or regional enforcement offices are responsible for the investigation and removal of FNs who are in violation of the IRPA, whether that is because they did not obtain the required authorisation prior to working in Canada, or because they remained in Canada beyond the period authorised for their stay. More specifically, inland enforcement officers will investigate FNs who are suspected or alleged to be working illegally, they will work to obtain the appropriate removal order, they will detain where necessary, and will oversee the removal of the person concerned. Where the FN or the party employing that FN has engaged in activity that constitutes an offence under the IRPA, the CBSA Criminal Investigations Program (CIP) will undertake a criminal investigation, prepare and lay the relevant charges under the IRPA, and work with the Public Prosecution Service of Canada to secure a conviction for the offence or offences committed. The CBSA CIP may also investigate and prosecute any other parties to an offence, such as immigration consultants who counsel misrepresentation or otherwise facilitate TFWP fraud. The CBSA Intelligence Operations and Analysis Division (IOAD) provides intelligence support to the immigration enforcement and criminal investigations programs by collecting, assessing, and disseminating information about suspected or actual contraventions of border-related legislation and programs, including the IRPA and TFWP.

D. Previous Privacy Impact Assessment and Historical Sharing of Information

Historically, the CBSA and ESDC have shared information regarding FNs, employers, and third parties, as reflected in the 2011 CBSA TFWP PIA. Sharing of information was conducted pursuant to subsection 34(1) of DESDA which provides ESDC with the authority to make personal information available to CBSA for the administration or enforcement of sections 82 and 203 of the IRPR.

The CBSA has historically shared information with ESDC regarding pending criminal prosecutions of individuals and companies, which assist ESDC in assessing current and future LMIAs.

Although the 2011 PIA recommended that the limited historical information sharing between ESDC and the CBSA be formalized, a Letter of Understanding (LOU) was not signed by the respective parties until

May 2014. Subsequently, an Information Sharing Agreement (ISA) was negotiated and signed in April 2015, to reflect an amendment to the DESDR that would expand information sharing between the two parties. This PIA reflects the changes introduced by the regulatory amendment and the ISA.

E. Overall Changes/Effect on the CBSA

In Economic Action Plan 2013, the Government of Canada committed to reforming the TFWP by protecting foreign workers from abuse and exploitation, and reinforcing the principle that Canadians be given the first chance to be selected for available jobs. The 2014 Budget committed significant funding for ESDC to make changes to the LMIA process and introduce reforms relating to LMIA-exempt situations. The reforms to the TFWP are aimed at:

- reducing employer use and reliance on temporary foreign workers (TFWs);
- Ensuring that employers who abuse the Program face significant consequences;
- Restricting access to the Program; and,
- Improving labour market information.

As part of these initiatives, ESDC will be investing more time and money into identifying and deterring employer misconduct with the TFWP conditions. In addition, both CIC and ESDC intend to increase their inspection activities and to seek authority to compel documents from third parties that could prove employer non-compliance. As a result, referrals to the CBSA for potential criminal investigation are expected to increase.

To facilitate information sharing, the two departments agreed to work together to amend the DESDR to recognize CBSA as a prescribed federal institution for the purposes of section 35 of DESDA (i.e. a law enforcement body recognized in the Act), which would allow ESDC to disclose data to the CBSA for the broader administration and enforcement of the IRPA. The relevant sections of the DESDA and DESDR are as follows:

Section 35(1) of the DESDA states: “[i]nformation may be made available to a minister or a public officer of a prescribed federal institution for the administration or enforcement of a prescribed federal or provincial law or activity if the Minister considers it advisable and the information is made available subject to conditions that are agreed on by the Minister and the federal institution.”

Section 3 of the DESDR states: For the purpose of subsection 35(1) of the Act, information that is obtained, or prepared from information that is obtained, under any program other than the Canada Pension Plan or the *Old Age Security Act* may be made available to the following...”

(a) the Canada Revenue Agency, for the administration or enforcement of the *Income Tax Act*;

...

(i) the Canada Border Services Agency, for the administration or enforcement of the *Immigration and Refugee Protection Act*.”

F. Information Sharing Agreement (ISA) Between ESDC and the CBSA

The final version of the ISA, which is attached as Annex J, came into force on April 16, 2015.

Details on the types of information to be exchanged between ESDC and the CBSA are described in Section 3 (Purpose of the ISA).

The ISA formalizes the exchange of information between the two institutions, including ample privacy protection clauses consistent with TBS's *Guideline on Preparing Information Sharing Agreements Involving Personal Information*, and describes the specific personal information which will be shared, as well as the manner in which it will be shared, as follows:

1. Disclosure of ESDC Information to CBSA

Personal information may be disclosed to the CBSA for the administration and enforcement of the TFWP and the IRPA. This includes, but may not be limited to, the issuance of work permits, determinations of admissibility, immigration and criminal investigations, and the development of intelligence products.

Annex C of the ISA (Section 2) lists the data elements which may be disclosed by ESDC upon request of the CBSA, or on ESDC's own initiative.

ESDC may disclose to the CBSA the personal information listed in Annex C, Section 2, and Annex D, Section 2 of the ISA, under section 35(1) of the DESDA.

2. Disclosure of CBSA Information to ESDC

In addition to the CBSA receiving information from ESDC, the Agency may disclose data to ESDC under the newly signed ISA.

In accordance with the ISA, the CBSA may provide information to ESDC for the purpose of administering and enforcing the TFWP and other activities assigned to ESDC under the IRPA and the IRPR. Annex E, Sections 2.1 through 2.3 of the ISA provides the data elements that may be disclosed to ESDC by the CBSA upon request, or on its own initiative, as appropriate, for the purpose of assessing LMIA requests, reviewing LMIAs, and conducting inspections under the IRPR.

The CBSA will endeavour to inform ESDC prior to undertaking public communication activities related to a TFWP-related criminal investigation.

G. Methods of Sharing Information (ESDC and CBSA)

The ISA between ESDC and the CBSA stipulates that information may be shared through system interfaces or through other means. Specifically, the information will be shared as reflected in the table below and depicted in Figure 1.

Table 2: Method of Delivery for Information Exchange

Method of Delivery	ESDC to CBSA	CBSA to ESDC
1. System Interface (FWS-GCMS) – See description below	Yes	No
3. Secure Courier (Hard Copies)	Yes	Yes

ESDC will share information with the CBSA primarily through the [redacted] When required information is unavailable through this view-only access, the information will be made available through secure courier,

The [redacted] will be established to allow for [redacted] relevant personal information. ESDC will maintain the [redacted] and CBSA will have access to it in order to deposit or extract information as set out in the ISA. Information will be [redacted] on a case-by-case basis as requested by either organization. The requesting organization will be notified via email that the files have been [redacted] and that the requestor has [redacted] to download them; after which the files will be deleted. The FTP site will be protected from unauthorized access by using [redacted] capability to access and use the [redacted] Approved users will be [redacted] to retrieve source files. ESDC will be capable of auditing the activity of all [redacted] users.

³ This delivery method is not depicted in Figure 1.

H. Information Systems

The following describes the ESDC and CBSA information systems utilized to support the ISA.

1. ESDC – Foreign Worker System (FWS)

The FWS is ESDC's single, integrated system used internally to process applications for LMIA's and to track employer compliance with Program requirements. The FWS stores only the types of personal information required to process LMIA's and conduct assessments of employer compliance. The type of personal information collected includes, but is not limited to:

- Client identification: family name, given names, gender, date of birth (DOB), country of birth (COB), etc.
- Contact information, including history
- Job offer information
- Compliance history, etc.

As reflected in Figure 1 above, the FWS maintains an interface with FOSS and GCMS both of which are systems maintained by CIC and for which CBSA staff have various user rights profiles.

2. ESDC – SharePoint

ESDC maintains a SharePoint site which stores various types of data that may be of benefit to a CBSA investigation or intelligence effort. For example, information received via ESDC's Online Fraud Reporting Tool (See Section 4.3 of this PIA) is stored in SharePoint. Data, reports, or forms that are stored on SharePoint may be shared by ESDC in accordance with the ISA.

3. CBSA – Field Operational Support System (FOSS)

FOSS is CIC's ageing immigration system. At the writing of this PIA, an interface to FOSS remains, but will be replaced by an interface to GCMS prior to the decommissioning of FOSS.

FOSS and GCMS exist in parallel to ensure that both systems maintain accurate data. An interface exists between FOSS and GCMS sharing transactional data to ensure both systems maintain similar data until FOSS is decommissioned.

Until such time that FOSS is decommissioned, the FWS-FOSS and FWS-GCMS interfaces will remain. The FWS-FOSS interface will cease when FOSS is decommissioned, expected by December 2015.

4. CBSA – Global Case Management System (GCMS)

The GCMS is CIC's single, integrated and worldwide system used internally to process applications for citizenship and immigration services. GCMS stores only the type of personal information required to process citizenship and immigration clients. The type of personal information collected includes, but is not limited to: client identification, contact information and educational and employment information.

CBSA has various user rights within GCMS; mostly "view only" access. The FWS-FOSS and FWS-GCMS interface allow CBSA users view only access to FWS data. The interface does not support FOSS or GCMS data being transmitted to FWS.

5. CBSA – Integrated Customs Enforcement System (ICES)

The Integrated Customs Enforcement System (ICES) is the CBSA's primary customs enforcement system at POEs. As such, ICES is the repository for enforcement-related information. This includes records of seizures and other enforcement actions, lookouts, intelligence, and information from external sources relating to enforcement.

ICES provides enforcement action data capture, lookout creation and dissemination, query and reporting available 24/7, 365 days a year. All information contained within ICES is classified as Protected B.

ICES also includes information on traveller history and vehicle passage history which enables the CBSA to fully measure, evaluate and report on the performance of the enforcement program and its related activities.

ICES is designed to support both the front line officers and the intelligence and investigations resources' ability to collect, analyze and disseminate the information necessary to identify and react to border-related risks.

Information regarding FNs seeking entry to Canada, including those seeking entry under the TFWP and FSWP, may be stored in ICES. As such, it may be referenced when sharing information with ESDC.

6. National Case Management System (NCMS)

The National Case Management System (NCMS) is the CBSA's primary immigration enforcement case management system which interfaces with FOSS and GCMS. Dedicated to serving the needs of Immigration Enforcement Officers, NCMS is a web-enabled immigration enforcement case tracking tool that tracks approximately 1,000 new enforcement cases per week. The database contains over 150,000 active enforcement cases and more than 500,000 historical records.

7. CBSA – Criminal Investigation Information Management System (CIIMS)

CIIMS is the principal information management system used by employees in the CBSA's CIP. CIIMS is an information management, as opposed to a case management system.

CIIMS is scheduled to be replaced by an information/case management system in FY 2016-17.

8. CBSA – Intelligence Management System (IMS)

Information shared by ESDC may be provided to CBSA's HQ and regional intelligence units, which store all information/intelligence in their dedicated case management application; the IMS. Access to the IMS is restricted to IOAD staff, regional intelligence units, the National Security Screening Division, the Border Operations Centre, National Targeting Centre, and CIP. Some of these units have read only access. For the purposes of fulfilling its mandate some IOAD data is disclosed to BSOs, IEOD or other internal and external partners.

It is further noted that some users, such as BSOs and IEOD, have some access to IMS through the Occurrence Reporting System (ORS), which enables them to input data to IMS, but prohibits them from viewing any data. These same users are able to utilize ORS to query IMS, which

presents a “hit list” for their subject query. These users must contact an IO for further details on the “hit list”.

9. Secure Tracking System (STS)

The Secure Tracking System (STS) contains information regarding FNs who have had a security screening check completed, or have one underway as a result of an application to enter Canada. In some instances, STS may contain information on FN's involved in and/or associated with any organization involved in war crimes, crimes against humanity and/or terrorist activities, organized crime, money laundering, terrorist financing, human smuggling, or persons associated with criminal organizations, and whose admission or presence in Canada may be contrary to immigration or citizenship legislation.

The primary role of STS is to assist in screening Temporary and Permanent Resident (TR/PR) visa applications.

STS has a full text storage capability that contains information gathered by intelligence units including Canadian and foreign investigative bodies and law enforcement agencies. The system tracks individuals, their actions and associations. It enables the exchange of screening requests between missions and HQ, and assists in vetting all visitors and groups seeking to come to Canada or those already in Canada as visitors, as TR, PR, or naturalized citizens known to or suspected of engaging in activities contrary to the IRPA. The information contained in STS may be used in the administration of immigration legislation.

In limited circumstances, IOAD and regional intelligence units may store information collected from ESDC in STS.

10. User Rights and Audit Trails Within CBSA Systems

The CBSA systems described above include a variety of security features to protect the sensitive information that is stored within them. Access to various sections within the systems is granted on a “profile” basis. The profile assigned to a user dictates which sections of the application the user can access, as well as what information can be viewed or edited. The systems described above also utilize a detailed audit trail that keeps track of the dates and times users’ access, edit and view the various records.

I. Scope of this PIA

The scope of this PIA is limited to CBSA activities that fall under the ISA between the CBSA and ESDC. It is intended to complement a parallel PIA being authored by ESDC on the ISA. While the ESDC PIA addresses the Department’s regulatory reform to support information sharing and the ISA, the CBSA’s PIA is limited in scope to the manner in which the CBSA will request, use, store, protect and disclose information under the ISA.

SECTION 1 - OVERVIEW AND INITIATION

Report Objectives

This report is a PIA regarding the ISA between the CBSA and ESDC. The objectives of this PIA are:

- to review the business processes in order to identify the data flow of personal information;
- to analyze the collection, use, disclosure and retention of personal information;
- to determine if there are privacy risks associated with the ESDC information exchange; and
- to provide recommendations on the mitigation or elimination of the risks.

The information presented in this report follows the TBS Directive on Privacy Impact Assessment and its related directives and guidelines.

The purpose of a PIA process is to ensure that privacy is considered throughout the project development cycle. The results of a PIA are a documented guarantee that privacy issues have been identified and adequately addressed.

Government Institution: Canada Border Services Agency, Programs Branch

Government Official Responsible for the Privacy Impact Assessment

Peter Hill
 A/Vice President, Programs Branch

Head of the government institution / Delegate for section 10 of the Privacy Act

Dan Proulx
 Director, Access to Information and Privacy (ATIP)

Name of Program or Activity of the Government Institution:

Temporary Foreign Worker Program (TFWP)

Description of Program or Activity:

Program 1.4: Criminal Investigations

Under the Criminal Investigations Program, the CBSA protects the integrity of border-related legislation and contributes to public safety and Canada's economic security by investigating and pursuing the prosecution of persons who commit criminal offences in contravention of Canada's border-related legislation.

CBSA investigators review potential border legislation violations and gather evidence using a variety of investigative techniques, including search warrants and production orders. These violations include criminal offences under the Customs Act, Immigration and Refugee Protection Act, various food/plant and animal legislation, and other border-related legislation. In conjunction with the Public Prosecution Service of Canada, the CBSA pursues the prosecution of individuals or business entities who violate Canada's border-related legislation.

Program 1.5: Immigration Enforcement

The Immigration Enforcement Program determines whether foreign nationals and permanent residents who are or may be inadmissible to Canada are identified and investigated, detained, monitored and/or removed from Canada.

Foreign nationals and permanent residents of Canada believed to be inadmissible are investigated and may have a report written against them by a CBSA inland enforcement officer. Depending on the type of inadmissibility, the merits of the report are reviewed by either a Minister's delegate or an independent decision maker at the Immigration and Refugee Board of Canada (IRB) where a CBSA hearings officer represents the Minister of Public Safety and Emergency Preparedness. Subsequent to this review, a removal order may be issued against the foreign national or permanent resident in question. Removal orders issued against refugee claimants are conditional and do not come into force until the claim is abandoned, withdrawn or denied by the IRB.

Description of the class of records (CORs) associated with the program or activity:

Description: Describes records related to the Temporary Foreign Worker Program. May include records related to the use of electronic systems used to administer or manage the program including the Citizenship and Immigration Canada's Field Operations Support System (FOSS), Computer-Assisted Immigration Processing System (CAIPS), and the National Case Management System (NCMS).

Class of Record Number: CBSA ADM 135

- ☐ Proposal for a New Personal Information Bank
- ☐ Proposal to modify an existing Personal Information Bank - identify PIB registration number and current description:

Temporary Foreign Worker Program (CBSA PPU 050)

Description: This bank describes information that is related to the administration of the Temporary Foreign Worker Program. The personal information may include name, aliases, contact information, biographical information, citizenship status, criminal checks/history, date of birth, gender, educational information, employee identification number, passport number, client identification number, work permit number, temporary visa number, other identification numbers, language, medical information, physical attributes, place of birth, signature and last country of residence.

Note: In addition to the requirements specified on the Treasury Board of Canada Secretariat Personal Information Request form, individuals requesting information described by this bank must provide the Name, aliases, date of birth, Client identification number (also known as Field Operations Support System (FOSS) number, work permit number, citizenship. Information may be stored in the following internal systems / databases: Field Operational Support System (FOSS), Global Case Management System (GCMS), Computer Assisted Immigration Processing System (CAIPS).

There are two related PIBs and CORs for Criminal Investigations and Intelligence. Those are reflected below:

Description of the CORs associated with the program or activity:

Description: Describes records related to the investigation of individuals and entities suspected of committing offences against Canada's border legislation, such as the Customs Act and/or the Immigration and Refugee Protection Act (IRPA), and any subsequent or related prosecution.

Note: Records may be found in the following systems: Criminal Investigations Information Management System (CIIMS), the Intelligence Management System (IMS), the Integrated Customs Enforcement System (ICES), the Field Operations Support System (FOSS), the National Case Management System (NCMS), the Global Case Management System (GCMS), the Automated Import Reference System (AIRS), the Accelerated Commercial Release Operations Support System (ACROSS) and the Canadian Police Information Center (CPIC).

Class of Record Number: CBSA ENF 123

Criminal Investigations Program (CBSA PPU 1402)

Description: This bank describes information that is about individuals subject to criminal investigation by the CBSA. Personal information may include photographs, name, contact information, biographical information, biometric information, citizenship status, credit information, criminal checks/history, date of birth, date of death, educational information, financial information, personal identification numbers, physical attributes, place of birth, place of death, signature, identity/travel document, residence history, phone records, computer records, caution flags, business records, import/export information, customs infractions and seizures, immigration violations and offences, travel history.

Note: In addition to the requirements specified on the Treasury Board of Canada Secretariat Personal Information Request form, individuals requesting information described by this bank must provide the incident and location. Personal information may be stored in the following systems: the Criminal Investigations Information System (CIIMS), the Intelligence Management System (IMS), the Integrated Customs Enforcement System (ICES), the Automated Import Reference System (AIRS), the Accelerated Commercial Release Operations Support System (ACROSS), the Field Operations Support System (FOSS), the Global Case Management System (GCMS), the National Case Management System (NCMS), the Secure Tracking System (STS) and the Canadian Police Information Centre (CPIC).

Description of the CORs associated with the program or activity:

Description: Describes records related to intelligence activities concerning individuals and entities that are of interest to the CBSA in connection to smuggling and contraband, irregular migration, immigration fraud, and inadmissibility and terrorism in support of CBSA's border enforcement mandate.

Note: Records may be found in the following systems: the Intelligence Management System (IMS), the Support System for Intelligence (SSI), the Integrated Customs Enforcement System (ICES), the Field Operations Support System (FOSS), the National Case Management System (NCMS), the Global Case Management System (GCMS) and the Canadian Police Information Center (CPIC).

Class of Record Number: CBSA ENF 1401

Intelligence Program (CBSA PPU 035)

Description: This bank describes information that is about individuals suspected of involvement in contraband smuggling, money laundering, terrorist financing, immigration fraud, irregular migration, human smuggling and/or trafficking, terrorism, or other border related enforcement and security concerns. Also includes information on individuals suspected of being inadmissible to Canada. Personal information may include name, contact information, biographical information, biometric information, citizenship status, credit information, criminal checks/history, date of birth, educational information, financial information, travel/identity documents, personal identification numbers, physical attributes, place of birth, signature, import/export information, customs infractions and/or seizures, traveller history and immigration violations.

Note: In addition to the requirements specified on the Treasury Board of Canada Secretariat Personal Information Request form, individuals requesting information described by this bank must provide the incident and location. Personal Information may be stored in the following systems: the Intelligence Management System (IMS), the Support System for Intelligence (SSI), the Secure Tracking System (STS), the Integrated Customs Enforcement System (ICES), the National Case Management System (NCSM), the Field Operations Support System (FOSS), the Global Case Management System (GCMS) and the Canadian Police Information Center (CPIC).

- ☐ Proposed new Standard Personal Information Bank
- ☐ Proposal to modify an existing Standard Personal Information Bank - identify Standard PIB number and current description:

N/A

Legal Authority for Program or Activity:

With respect to the CBSA-EDSC TFWP ISA, personal information is collected pursuant to Sections 11, 20 and 22 of the *Immigration and Refugee Protection Act* (IRPA) and Part 11 of the *Immigration and Refugee Protection Regulations* (IRPR).

In addition to what is identified in the ISA, personal information is also collected by the CBSA under sections 15, 16, and 18 of the IRPA and s. 5 of the *CBSA Act*.

Also, Pursuant to paragraph 8(2)(a) of the *Privacy Act*, and under section 209.92 of IRPR, the CBSA has the authority to disclose information related to the TFWP to ESDC for the administration or enforcement of the TFWP, the FSWP and the IMP.

Summary of the project, initiative, or change:

The TFWP enables employers to hire TFWs as a last resort to meet their short-term labour and skills needs when qualified Canadian citizens or permanent residents are not available, while respecting international trade agreements and other partnerships. The FSWP is a pathway to permanent residence for high skilled foreign nationals who are looking to become established in Canada. The TFWP and FSWP are jointly managed by ESDC and CIC under the authority of the IRPA and IRPR.

The LMIA (issued by ESDC) determines whether the employment of a TFW is likely to have a positive or negative effect on the Canadian labour market. Information collected and used for this assessment includes: employer business and personal information, TFW personal information and employer compliance information (including Employer Compliance Review (ECR) or Inspection results). ESDC also issues LMIAs for permanent resident applicants under the FSWP.

The IMP, managed by CIC under the authority of the IRPA and IRPR, includes streams of work for which an LMIA is not required. Its primary objective is to advance Canada's broad economic and cultural natural interest, rather than filling a particular job.

The CBSA's role in the TFWP, FSWP and IMP includes determining the admissibility of foreign nationals to Canada and determining whether to issue work permits at POE. The CBSA is also responsible for investigating cases of possible criminal activity under the IRPA, ranging from misrepresentation by an employer on an LMIA application (i.e. false, misleading or fraudulent information) to locating and removing FNs, including TFWs, who are in contravention of Canada's immigration legislation.

ESDC has amended the DESDR to identify the CBSA as an organization to which information can be disclosed under s. 35(1) of the DESDA. Prior to the regulatory amendment, ESDC could only share information with the CBSA pursuant to subsection 34(1).

In April 2015, an ISA was signed between ESDC and the CBSA to enumerate the personal information which may be exchanged between the two departments. The ISA is attached to this PIA as Annex J.

SECTION 2 - RISK AREA IDENTIFICATION AND CATEGORIZATION

Type of Program or Activity

Level of Risk

Program or activity that does NOT involve a decision about an identifiable individual

☐ 1

Personal information is used strictly for statistical / research or evaluations including mailing list where no decisions are made that directly have an impact on an identifiable individual.

The Directive on PIA applies to administrative use of personal information. The Policy on Privacy Protection requires that government institutions establish an institutional Privacy Protocol for addressing non-administrative uses of personal information. The CBSA Privacy Protocol must be implemented. Contact the ATIP Division before continuing the PIA.

Administration of Programs / Activity and Services

☒ 2

Personal information is used to make decisions that directly affect the individual (i.e. determining eligibility for programs including authentication for accessing programs/services, administering program payments, overpayments, or support to clients, issuing or denial of permits/licenses, processing appeals, etc...).

Compliance / Regulatory investigations and enforcement

☒ 3

Personal information is used for purposes of detecting fraud or investigating possible abuses within programs where the consequences are administrative in nature (i.e. a fine, discontinuation of benefits, audit of personal income tax file or deportation in cases where national security and/or criminal enforcement is not an issue).

Criminal investigation and enforcement / National Security

☒ 4

Personal information is used for investigations and enforcement in a criminal context (i.e. decisions may lead to criminal charges/sanctions or deportation for reasons of national security or criminal enforcement).

Details: Information collected by the CBSA will be used to make a decision that directly affects the individual (admissibility and eligibility in the TFWP/FSWP; detention, removal from Canada, and prosecution – which may lead to loss of freedom). Also, employers and relevant third parties (i.e. Consultants) may be investigated by the CBSA for alleged offences under IRPA.

Type of Personal Information Involved and Context

Level of Risk

Only personal information, with no contextual sensitivities, collected directly from the individual or provided with the consent of the individual for disclosure under an authorized program. For example: General licensing, or renewal of travel documents or identity documents.

☐ 1

Personal information, with no contextual sensitivities after the time of collection, provided by the individual with consent to also use personal information held by another source. For example: An application process with a requirement for independent verification of certain non-sensitive factual details.

☒ 2

Social Insurance Number, medical, financial or other sensitive personal information and/or the context surrounding the personal information is sensitive. Personal information of minors or incompetent individuals or involving a representative acting on behalf of the individual. For example: An individual's name on a particular list may reveal sensitive information on the health, financial situation, religious or lifestyle choices of that individual.

☒ 3

Sensitive personal information, including detailed profiles, allegations or suspicions, bodily samples and/or the context surrounding the personal information is particularly sensitive. For example: Personal information that reveals intimate details on the health, financial situation, religious or lifestyle choices of the individual and which, by association, reveals similar details about other individuals such as relatives.

☒ 4

Details: Information collected by the CBSA for administration of the TFWP/FSWP, which involves the collection and use of information provided on LMIA, WP, and visa application forms. Also, information is collected and used to support criminal investigations, which often contain information/allegations that are of a sensitive or highly sensitive nature.

Program or Activity Partners and Private Sector Involvement

Level of Risk

Within the CBSA (amongst one or more programs within the CBSA)

☒ 1

With other federal institutions

☒ 2

With other or a combination of federal/ provincial and/or municipal government(s)

☒ 3

Private sector organizations or international organizations or foreign governments

☐ 4

Details: Within the CBSA information will be used by BSOs, investigators, intelligence officers and analysts within the CIP, IEOD, and IOAD, as well as regional investigations units. Also, information will be exchanged with ESDC to support administration of the TFWP by both departments.

Information may be provided by the CBSA to federal, provincial, or territorial courts, the IRB, as well as the Public Prosecution Service of Canada, to support the issuance of search warrants, Production Orders, and in relation to criminal prosecution and removals.

Duration of the Program or Activity

Level of risk

One time program or activity

☐ 1

Typically involves offering a one-time support measure in the form of a grant payment as a social support mechanism.

Short-term program

☐ 2

A program or activity that supports a short-term goal with an established "sunset" date.

Long-term program

☒ 3

Existing program that has been modified or is established with no clear "sunset".

Details: The exchange of information is intended to be a long-term agreement with no clear sunset.

Program Population

Level of Risk

The program affects certain employees for internal administrative purposes.

☐ 1

The program affects all employees for internal administrative purposes.

☐ 2

The program affects certain individuals for external administrative purposes.

☒ 3

The program affects all individuals for external administrative purposes.

☐ 4

Details: The information collected and used by the CBSA will affect individuals (FNs, third parties) and companies for the administrative purpose of determining eligibility for the TFWP, FSWP, IMP, admissibility to Canada, and compliance with the IRPA, which may result in criminal prosecution related to contraventions of the IRPA.

Technology and Privacy

6.1 Does the new or modified program or activity involve the implementation of a new electronic system, software or application program including collaborative software (or groupware) that is implemented to support the program or activity in terms of the creation, collection or handling of personal information?

☒ YES

☐ NO

6.2 Does the new or modified program or activity require any modifications to IT legacy systems and / or services?

☐ YES

☒ NO

6.3 Does the new or modified program or activity involve the implementation of one or more of the following technologies:

6.3.1 Enhanced identification methods:

☐ YES

This includes biometric technology (i.e. facial recognition, gait analysis, iris scan, fingerprint analysis, voice print, radio frequency identification (RFID), etc...) as well as easy pass technology, new identification cards including magnetic stripe cards, "smart cards" (i.e. identification cards that are embedded with either an antenna or a contact pad that is connected to a microprocessor and a memory chip or only a memory chip with non-programmable logic).

☒ NO

Details:

6.3.2 Use of Surveillance:

☒ YES
☐ NO

This includes surveillance technologies such as audio/video recording devices, thermal imaging, recognition devices, RFID, surreptitious surveillance / interception, computer aided monitoring including audit trails, satellite surveillance etc.

Details: CBSA regional criminal investigations offices conduct surveillance operations in support of on-going TFWP investigations. Surveillance operations of the CBSA are limited to those directly within the CBSA's border management mandate and are undertaken for the purpose of obtaining information. Information may be obtained through direct observation as well as through the use of audio and/or visual recording equipment.

6.3.3 Use of automated personal information analysis, personal information matching and knowledge discovery techniques:

☐ YES
☒ NO

For the purposes of the Directive on PIA, CBSA is to identify those activities that involve the use of automated technology to analyze, create, compare, cull, identify or extract personal information elements. Such activities would include personal information matching, record linkage, personal information mining, personal information comparison, knowledge discovery, information filtering or analysis. Such activities involve some form of artificial intelligence and/or machine learning to uncover knowledge (intelligence), trends/patterns or to predict behaviour.

Details:

Details: The CBSA will upload data TFWP/FSWP information with the CBSA will be stored for a limited time to retrieve source files as per the ISA.

which will be administered by the ESDC. ESDC will share as well. The site will utilize and data Approved user(s) will be given access codes to ESDC's

Personal Information Transmission

Level of Risk

The personal information is used within a closed system.

☐ 1

No connections to Internet, Intranet or any other system. Circulation of hardcopy documents is controlled.

The personal information is used in system that has connections to at least one other system.

☒ 2

The personal information is transferred to a portable device or is printed.

☒ 3

USB key, CD-Rom, laptop computer, any transfer of the personal information to a different medium.

The personal information is transmitted using wireless technologies.

☐ 4

Details: Personal information will be provided by ESDC to the CBSA in four methods: a one way interface from

Personal information will be disclosed by the CBSA to ESDC using three methods:

Risk Impact to the CBSA

Level of Risk

Managerial harm.

☒ 1

Processes must be reviewed, tools must be changed, change in provider / partner.

Organizational harm.

☒ 2

Changes to the organizational structure, changes to the organizations decision-making structure, changes to the distribution of responsibilities and accountabilities, changes to the program activity architecture, departure of employees, reallocation of HR resources.

Financial harm.

☒ 3

Lawsuit, additional moneys required reallocation of financial resources.

Reputation harm, embarrassment, loss of credibility.

☒ 4

Decreased confidence by the public, elected officials under the spotlight, institution strategic outcome compromised, government priority compromised, impact on the Government of Canada Outcome areas.

Details: Decreased confidence from the public and potential lawsuits by the public if there is a privacy breach of exposing personal information. A privacy breach could compromise public confidence in the CBSA, compromise ongoing investigations, or could jeopardize our relationship with external and international partners, all of which may impact the CBSA's priorities and ultimately the Government of Canada as a whole.

The loss of information via a privacy breach could have a reputational harm to the CBSA and ESDC, which may decrease public confidence in the institutions' ability to deliver its mandate and collect, use, and store personal information in an appropriate manner.

Risk Impact to the Individual or Employee

Level of Risk

Inconvenience.

☒ 1

Reputation harm, embarrassment.

☒ 2

Financial harm.

☒ 3

Physical harm.

☒ 4

Details: The loss of information via a privacy breach could affect individuals across all four levels of risk. The data that is collected and shared by the CBSA and ESDC may be highly sensitive and could result in instance of reputational harm and/or identity theft if a breach were to occur. In some instances, when tips are received, ESDC asks the individual if he/she will be in imminent danger or risk of serious physical injury. People who fear for their safety due to employer threats, physical harm may be a possibility.

SECTION 3 - ANALYSIS OF PERSONAL INFORMATION ELEMENTS

Personal Information Elements and Sub-elements

The various personal information elements collected by the Program fall under two broad categories, being:

- **Table 3: Personal Information Disclosed by ESDC to the CBSA** The information in this table is taken verbatim from the information specified as being disclosed by ESDC to the CBSA in Annexes C and D of the ESDC-CBSA TFWP ISA.
- **Table 4: Personal Information Disclosed by the CBSA to ESDC.** The information in this table, and the paragraph that precedes this table, is taken verbatim from the information specified as being disclosed by the CBSA to ESDC in Annex E of the ESDC-CBSA TFWP ISA.

Table 3: Personal Information Disclosed by ESDC to the CBSA

Data Elements	Reason for which data element is collected, used and/or disclosed	From:	To:
Business Information			
*Employer ID	Internal number assigned to identify employer in the foreign worker system(FWS)	ESDC	CBSA
*Employer CRA BN	To confirm that the employer has a registered business	ESDC	CBSA
*Employer business and legal name	To identify the employer's business name	ESDC	CBSA
*Employer mailing address, including street number, city, province, postal code, phone number and fax number.	For correspondence with the employer on LMIA decisions and inspections	ESDC	CBSA
*Employer business address (if different than mailing address), including street number, city, province, postal code	Secondary contact information to correspond with the employer in case of inspections or questions on the LMIA	ESDC	CBSA
Type of Business		ESDC	CBSA
Response to Question: Is the		ESDC	CBSA

Table 3: Personal Information Disclosed by ESDC to the CBSA

Data Elements	Reason for which data element is collected, used and/or disclosed	From:	To:
business a franchise?			
Response to Question: If the business is a franchise, is the corporate head office aware of this application for TFWs?		ESDC	CBSA
*Website address	To verify contact information provided on the LMIA application if necessary	ESDC	CBSA
*Date business started	To assess the employer's legitimacy and ability to fulfil the terms and conditions of employment	ESDC	CBSA
*Describe the main business activity	To determine the occupation and corresponding NOC code and labour shortage for that occupation	ESDC	CBSA
*Principal contact name	To establish name of the employer for contact purposes	ESDC	CBSA
*Telephone number + extension if applicable, fax number and e-mail address	To contact employer	ESDC	CBSA
*Contact Job Title	To determine the occupation and corresponding NOC code and to identify the prevailing wage for the requested position	ESDC	CBSA
*Preferred Official Language of Correspondence	To ensure that correspondence with employer is in the correct language	ESDC	CBSA
Third-Party, Recruiter or Employment Agency Information			
Response to Question: Are you using the services of a third-party, recruiter or employment agency for the purposes of hiring a TFW?		ESDC	CBSA
Name of third-party, recruiter or employment agency for the purposes of hiring a TFW	To identify the third party (third parties are often designated by the employer as the point of contact)	ESDC	CBSA
Registration, license or certificate		ESDC	CBSA

Table 3: Personal Information Disclosed by ESDC to the CBSA

Data Elements	Reason for which data element is collected, used and/or disclosed	From:	To:
number			
Response to Question: Are you appointing a third-party to represent you in completing this application form or to provide advice in and immigration process?		ESDC	CBSA
Name of third-party representative		ESDC	CBSA
Response to Question: Have you the employer or any other third-party in connection to this job offer received payment from the TFWs to secure this offer of employment?		ESDC	CBSA
Business Details			
Number of employees currently employed nationally under this CRA Business number	To assess the genuineness of the employer and protection of the labour market (ensure that the employer is not favouring TFWs over Canadians and permanent residents).	ESDC	CBSA
Total number of employees currently employed at the work location specified on this form	To assess the genuineness of the employer and protection of the labour market (ensure that the employer is not favouring TFWs over Canadians and permanent residents).	ESDC	CBSA
Number of Canadians/permanent resident employees at work location covered by this LMIA	To assess the number of TFWs in Canada that are currently employed by the employer	ESDC	CBSA
Total number of TFWs at the work location specified on this form	To assess the number of TFWs in Canada that are currently employed by the employer	ESDC	CBSA
Response to Question: Did you employ a TFW in the last two years, prior to December 31, 2013?		ESDC	CBSA

Table 3: Personal Information Disclosed by ESDC to the CBSA

Data Elements	Reason for which data element is collected, used and/or disclosed	From:	To:
Response to Question: Did you provide all TFWs employed by you in the last two years with wages, working conditions and employment in an occupation that were substantially the same as those that were described in the offer(s) of employment?		ESDC	CBSA
Response to Question: Have you applied for and received a positive LMIA on or after December 31, 2013?		ESDC	CBSA
Response to Question: Did you provide all TFWs employed by you, on all LMIA's received on or after December 31, 2013, with employment in the same occupation as described in the offer(s) of employment and with substantially the same wages, working conditions – but not less favourable than – those set out in that offer(s) of employment?		ESDC	CBSA
Response to Question: Have you had an LMIA revoked within the previous 2 years from the date you submitted the application?		ESDC	CBSA

Table 3: Personal Information Disclosed by ESDC to the CBSA

Data Elements	Reason for which data element is collected, used and/or disclosed	From:	To:
If yes, date and system file number			
Response to Question: Were any employees laid off in the past 12 months? If yes, how many? Reason(s) for layoff(s) and occupations affected	To ensure that the employer is not requesting a TFW for a position which a Canadian was laid off and cross-referencing the employer response with ROE employer information.	ESDC	CBSA
Response to Question: Does your business receive support through any Government of Canada program? If yes, name of program	To cross-reference whether or not the occupation(s) affected on the employer's Work-Sharing agreement match with the occupation(s) listed on the LMIA.	ESDC	CBSA
Job Offer Information			
*Job title	For officers to determine the appropriate NOC level for the position requested	ESDC	CBSA
Number of TFWs requested on this job offer	To determine the impact on the labour market and will be used to calculate the amount of the user fee for the LMIA.	ESDC	CBSA
*Expected duration of employment	To cross reference the duration of employment with the type of position requested (i.e. Seasonal occupation would not require a 2 year employment) and verify the duration for which the work permit was issued to the TFW	ESDC	CBSA
*Expected start date of employment, if any	To verify against the start date of the work permit issued to the TFW	ESDC	CBSA
*Location of job: Number and Street, city, province and postal code	To identify and ensure the location where the work will take place (i.e. an employer could have multiple locations for their business).	ESDC	CBSA
*Main duties of the job	For officers to determine: the occupation and corresponding NOC code	ESDC	CBSA
*Educational requirements of the job:	To assess if the TFW meets the educational requirements of the job. CIC will verify this when the TFW applies for a work permit	ESDC	CBSA
*Experience/skills requirements of	To assess if the TFW meets the skills requirements of the job. CIC will verify	ESDC	CBSA

Table 3: Personal Information Disclosed by ESDC to the CBSA

Data Elements	Reason for which data element is collected, used and/or disclosed	From:	To:
the job	this when the TFW applies for a work permit		
*Language requirements	To ensure that the language requirement of the job requested and advertised is either French or English or a rationale is provided for 'other' language	ESDC	CBSA
Wage in Canadian Dollars and number of work hours and overtime hours rate	To assess whether the wages offered to the TFW are consistent with the prevailing wage rate for the occupation and whether the working conditions meet generally accepted Canadian standards	ESDC	CBSA
Response to Question: Is the employment seasonal?		ESDC	CBSA
*Benefits	To assess whether the benefits offered to the TFW meet generally accepted Canadian standards	ESDC	CBSA
*Other benefits	To have comprehensive information on all the benefits provided, which can be verified during an inspection	ESDC	CBSA
*Response to Question: Are there provincial/territorial/federal certification, licensing or registration requirements of the job? If yes, name of the certifying/licensing/registering body	To assess if the TFW meets the certification/licensing/registration requirements of the job (CIC to verify when the TFW applies for a work permit)	ESDC	CBSA
Confirmation that the position is part of a union. If yes, name of the Union.	To verify wage(s) and benefits that apply. Where a collective bargaining agreement exists, the wages and benefits listed within will be used for assessment	ESDC	CBSA
Response to Question: Has the union been consulted about hiring a TFW? If yes, what is the position of the union?		ESDC	CBSA

Table 3: Personal Information Disclosed by ESDC to the CBSA

Data Elements	Reason for which data element is collected, used and/or disclosed	From:	To:
Response to Question: Have you attempted to recruit Canadians / permanent residents for this job?	For the officer to determine if the employer attempted to recruit Canadians and permanent residents for the job prior to applying for an LMIA. An employer must submit supporting documentation with the LMIA application to show proof of advertising; such as, advertisements in local and national newspapers, recognized internet job sites, job-specific and professional publications, recruitment drives, job fairs etc.)	ESDC	CBSA
Response to Question: What are the potential benefits to the labour market for offering this job to a TFW?	To determine whether the employment of the foreign national will or is likely to result in the development or transfer of skills and knowledge for the benefit of Canadian citizens or permanent residents. To determine whether the employment of the foreign national will or is likely to result in direct job creation or job retention for Canadian citizens or permanent residents	ESDC	CBSA
Rationale for the job offer to TFWs	For the officer to verify whether the employment of the foreign national is likely to fill a labour shortage	ESDC	CBSA
Response to Question: Do you plan to hire or train Canadians / permanent residents for the position for which you are requesting an opinion?	To determine whether the employer will hire or train Canadian citizens or permanent residents or has made, or has agreed to make, reasonable efforts to do so. For the officer to verify whether the employment of the foreign national will or is likely to result in direct job creation or job retention for Canadian citizens or permanent residents.	ESDC	CBSA
Summary of Results to Meet Minimum Recruitment and Advertising Requirements			
Number of applications/resumes received from Canadians/permanent residents		ESDC	CBSA

Table 3: Personal Information Disclosed by ESDC to the CBSA

Data Elements	Reason for which data element is collected, used and/or disclosed	From:	To:
Number of Canadians/permanent resident applicants interviewed		ESDC	CBSA
Number of Canadians/permanent residents offered the position		ESDC	CBSA
Number of Canadians/permanent residents hired		ESDC	CBSA
Number of job offers declined by Canadians/permanent resident applicants		ESDC	CBSA
Number of Canadians/permanent resident applicants who were not qualified for the job		ESDC	CBSA
Impacts on the Canadian Labour Market			
Response to Question: Will the entry of these TFWs lead to job losses, now or in the foreseeable future, for Canadians/permanent residents as a result of layoffs, outsourcing, offshoring or other factors related to utilizing TFWs?		ESDC	CBSA
Response to Question: Is the job offer related to an activity, contract or a subcontract that will facilitate outsourcing or offshoring?		ESDC	CBSA
Film and Entertainment Requests			
Name of Production	To identify the production by name	ESDC	CBSA
Total number of people involved in	To ascertain the size of the project	ESDC	CBSA

Table 3: Personal Information Disclosed by ESDC to the CBSA

Data Elements	Reason for which data element is collected, used and/or disclosed	From:	To:
the production			
Type of Production	To identify the type of the production to ensure that it does not contravene program requirements	ESDC	CBSA
Copy of the contract between the employer and the foreign entertainer(except for film and TV requests)	To verify the terms and conditions of the employment contract to ensure they meet program requirements and that they meet generally accepted Canadian labour standards	ESDC	CBSA
Temporary Foreign Worker Information			
Surname as shown on passport	To identify the TFW by name	ESDC	CBSA
Given name as shown on passport	To identify the TFW by name	ESDC	CBSA
Gender	To identify the TFW by gender	ESDC	CBSA
*Date of birth	To identify the TFW by DOB, especially for cases of multiple TFWs with the same name.	ESDC	CBSA
*Location of residence outside of Canada	For the officer to determine the TFW's immigration status and where the TFW is located in Canada	ESDC	CBSA
*Citizenship(s)	To identify the citizenship of TFWs	ESDC	CBSA
Location of TFW if in Canada and immigration Status	For the officer to determine the TFW's immigration status and where the TFW is located in Canada	ESDC	CBSA
Declaration of Employer			
Declaration of proprietorship	To identify if the employer is a sole proprietor or partnership and if 'yes', to determine whether or not their personal information can be shared with provinces for the provincial nominee program	ESDC	CBSA
Signature of employer and third party (if applicable)	To validate the employer signature against the LMIA request	ESDC	CBSA
Caregiver Program			
*Employer #1 and Employer #2	To address the employer when contacting him/her	ESDC	CBSA

Table 3: Personal Information Disclosed by ESDC to the CBSA

Data Elements	Reason for which data element is collected, used and/or disclosed	From:	To:
Given and last names			
*Employer #1 and Employer #2 Work and home telephone numbers	To contact the employer when clarification of LMIA application is needed and to make first contact when employer is selected for an inspection	ESDC	CBSA
*Employer #1 and Employer #2 Address: number/street/PO Box#	To correspond with the employer in case of inspections or questions on the LMIA	ESDC	CBSA
*Alternate contact person (spouse, common-law partner, other relative if applicable)	To correspond with the alternate contact when unable to contact the employer	ESDC	CBSA
*Given and last name of alternate contact	To address the alternate contact when contacting him/her	ESDC	CBSA
*Telephone number of alternate contact	To correspond with the alternate contact when unable to contact the employer	ESDC	CBSA
Caregiver Job Offer Information			
Number of dependents (including those that do not live in the household)	To assess a genuine need for a caregiver	ESDC	CBSA
Type of care required (foreign caregiver must provide care for at least one designated individual)	To assess a genuine need for a caregiver	ESDC	CBSA
Relationship of the employer to individual receiving care (i.e., child, elderly person, person with disability, chronic or terminal illness)	To assess a genuine need for a caregiver	ESDC	CBSA
Calculation of the financial ability of the employer	To assess the ability of the employer to pay the caregiver	ESDC	CBSA

Table 3: Personal Information Disclosed by ESDC to the CBSA

Data Elements	Reason for which data element is collected, used and/or disclosed	From:	To:
Will accommodation be provided at no charge? (attestation applies only if the caregiver will live and work in the same private household)	To assess the living conditions of the caregiver	ESDC	CBSA
Seasonal Agricultural Worker Program			
Total # of Canadian agricultural worker employed: • This year • Last year	For the officer to determine if there is an increase in the number of foreign workers requested compared to last year	ESDC	CBSA
Total # of foreign agricultural worker requested: • This year • Last year	For the officer to determine if there is an increase in the number of foreign workers requested compared to last year	ESDC	CBSA
If the requested number of workers is different from last year/season, please explain:	For the officer to determine if the change in the employer's labour needs is reasonable.	ESDC	CBSA
List crops/commodities, acreage, and method harvested	For the officer to determine the business activities of the employer	ESDC	CBSA
Housing type	To determine the type of housing provided (on-farm or off-site) and the weekly or monthly accommodations deductions. This can be verified during an employer inspection.	ESDC	CBSA
Housing inspection	If housing is provided, employers must provide proof that on-farm and/or off-site housing has been inspected by the appropriate provincial/territorial/municipal body or by an authorized private inspector. A negative LMIA may be issued if the employer does not provide: i) proof that the on-farm and/or off-site housing has been inspected, ii) a copy of the	ESDC	CBSA

Table 3: Personal Information Disclosed by ESDC to the CBSA

Data Elements	Reason for which data element is collected, used and/or disclosed	From:	To:
	contract between the employer and the facility dwelling), if applicable.		
Check one: Direct arrival, direct replacement, double arrival, double transfer, replacement transfer, double arrival, transfer	To determine type of position. Used for internal reporting purposes only.	ESDC	CBSA
Schedule A: Appointment of a Third-Party Representative			
Business Name	To identify the third party's business name	ESDC	CBSA
CRA Business Number	To confirm that the third party is a registered business	ESDC	CBSA
Legal Name	To identify the third party's legal name	ESDC	CBSA
Third-Party ID#	Internal number assigned to identify third party in the FWS	ESDC	CBSA
Mailing Address including street number, city, province, postal code, phone number and fax number.	For correspondence with the third party on LMIA decisions and inspections	ESDC	CBSA
Business Address including street number, city, province, postal code, phone number and fax number.	Secondary contact information to correspond with the third party in case of inspections or questions on the LMIA.	ESDC	CBSA
Main activity of the business	For officers to determine whether or not the services provided by the third party are legitimate.	ESDC	CBSA
Principal contact name	To verify that the third parties charging a fee for support with the LMIA application process are authorized and are one of the following: <ul style="list-style-type: none"> lawyers and paralegals who are members in good standing of a Canadian provincial or territorial law society Notaries who are members in good standing of the Chambre des notaires du Québec, and Immigration consultants who are members in good standing of the 	ESDC	CBSA

Table 3: Personal Information Disclosed by ESDC to the CBSA

Data Elements	Reason for which data element is collected, used and/or disclosed	From:	To:
	Immigration Consultants of Canada Regulatory Council		
Job Title	Job title associated with third party point of contact	ESDC	CBSA
Telephone Number	To contact the third party when clarification of LMIA application is needed	ESDC	CBSA
Fax Number	To mail the LMIA confirmation letter and corresponding annex	ESDC	CBSA
Email Address	A secondary point of contact for the third party if unable to reach by other means	ESDC	CBSA
Preferred Language of Correspondence	To ensure that correspondence with third party is in the correct language	ESDC	CBSA
Name of Employer Business		ESDC	CBSA
Response to Question: The representative is unpaid and:		ESDC	CBSA
Response to Question: The representative is, has been or will be paid and is a member of good standing of:		ESDC	CBSA
Schedule B: Impact on the Canadian Labour Market			
Name of Business		ESDC	CBSA
Employer Contact Name		ESDC	CBSA
Telephone Number		ESDC	CBSA
Alternate Telephone Number		ESDC	CBSA
Title		ESDC	CBSA
E-mail Address		ESDC	CBSA
Fax number		ESDC	CBSA
Name of Employer Applying for the LMIA		ESDC	CBSA
System File Number		ESDC	CBSA
Response to Question: Will the		ESDC	CBSA

Table 3: Personal Information Disclosed by ESDC to the CBSA

Data Elements	Reason for which data element is collected, used and/or disclosed	From:	To:
entry of TFWs lead to job losses, now or in the foreseeable future, for Canadians and/or permanent residents as a result of lay-offs, outsourcing, offshoring or other factors related to the utilizing TFWs?			
Response to Question: Does this contract or a subcontract facilitate outsourcing or offshoring?		ESDC	CBSA
Schedule C: Employer Transition Plan			
Business Name		ESDC	CBSA
CRA Business Number		ESDC	CBSA
Legal Name		ESDC	CBSA
Business Operating Name		ESDC	CBSA
Business Address including street number, city, province, postal code		ESDC	CBSA
Occupations of positions requested		ESDC	CBSA
Number of positions requested on the LMIA application		ESDC	CBSA
Number of Canadian/permanent resident employees currently employed in the occupation at the work location		ESDC	CBSA
Number of foreign workers currently employed in the occupation at the work location		ESDC	CBSA

Table 3: Personal Information Disclosed by ESDC to the CBSA

Data Elements	Reason for which data element is collected, used and/or disclosed	From:	To:
Total number of employees currently employed at the work location specified on the LMIA application		ESDC	CBSA
Number of employees currently employed nationally under this CRA business number		ESDC	CBSA
Seasonal occupation, if yes, peak employment season and total workforce during that time		ESDC	CBSA
Response to Question: Have you completed a Transition Plan for this occupation at this work location before? If yes, did the number of TFWs decrease relative to the number of Canadians/permanent resident workers for this occupation at this location as a result of activities conducted in the Transition Plan.		ESDC	CBSA
Description of planned activities		ESDC	CBSA
Proposed dates for activities		ESDC	CBSA
Results of planned activities		ESDC	CBSA
Actual results of activities		ESDC	CBSA
Milestones/benchmarks for activities, proposed and actual		ESDC	CBSA

Table 3: Personal Information Disclosed by ESDC to the CBSA

Data Elements	Reason for which data element is collected, used and/or disclosed	From:	To:
result: <ul style="list-style-type: none"> • Total number of applicants • Total number of applicant interviewed • Total number of positions offered • Total number of applicants hired 			
For each activity, rational for not hiring Canadians/permanent resident candidates		ESDC	CBSA
Foreign Caregiver Specific Genuineness Documents - data elements used for the genuineness assessments are listed below each document. While other data elements may exist on the document, employers are asked to redact all unnecessary information when submitting them as they are not used as part of the assessment.			
Pay Stub of applicant Personal information elements required (<i>all other elements redacted</i>): <ul style="list-style-type: none"> • Name of ER hiring caregiver • Remuneration paid 	Pay stubs are required to provide proof of salary. They indicate the weekly or yearly income and therefore contribute to substantiate the employer's financial situation. Applicants will be asked to submit 3 pay stubs from 3 different pay periods throughout a 12-month period.	ESDC	CBSA
Employer confirmation of salary	In absence of paystubs, applicants can submit a letter from their employer indicating their current salary and the number of years of service for said employer.	ESDC	CBSA
Confirmation of ability to pay from bank or notary	In absence of paystubs or employer confirmation, applicants can provide a letter from their bank or notary indicating their ability to pay the salary	ESDC	CBSA

Table 3: Personal Information Disclosed by ESDC to the CBSA

Data Elements	Reason for which data element is collected, used and/or disclosed	From:	To:
	required to hire a caregiver.		
Medical Disability Certificate Personal information elements required (all other elements redacted): <ul style="list-style-type: none"> Name of disabled person Address of disabled person Confirmation of Disability 	By this certificate, a medical doctor will attest that the individual identified as the person needing care in the LMIA is a disabled person, thus confirming the need for "care of a disabled person" category. Consent to release personal information from the person receiving care will be included on this certificate.	ESDC	CBSA
Old Age Security Card Personal information elements required (all other elements redacted): <ul style="list-style-type: none"> Name 	OAS card will provide evidence that the individual in need of care is a senior person. OAS card does not provide age, but is issued as per rigorous process insuring applicant is over 65 years or older. OAS is a good alternative to an unavailable birth certificate.	ESDC	CBSA
Passport (Senior Citizen) Personal information elements required (all other elements redacted): <ul style="list-style-type: none"> Name Date of birth 	Passport provides evidence of date of birth and name, thus confirming the need for care for the "senior home support care" category. . Can be requested as an alternative to birth certificate, but for senior people only. <u>Name:</u> to cross-reference with information provided in LMIA application/TFW System <u>Date of birth:</u> will provide evidence that the individual(s) in need of care is/are a senior person(s).	ESDC	CBSA
Long Form Birth Certificate (Mandatory for child, accepted for Senior citizen as proof of age) Personal information elements required (all other elements redacted): <ul style="list-style-type: none"> Name (last, given names) 	Long-form Birth Certificate provides evidence of date of birth, names of the child and of the parent(s), thus confirming need for care for the "child care" category. <u>Parent's Name(s):</u> to cross-reference with information provided in LMIA application/TFW System. Parent's name(s) on Birth Certificate must be same as Employer's name(s). <u>Child's name and date of birth:</u> will provide evidence that the individual(s) in	ESDC	CBSA

Table 3: Personal Information Disclosed by ESDC to the CBSA

Data Elements	Reason for which data element is collected, used and/or disclosed	From:	To:
<ul style="list-style-type: none"> • Date of birth • Parent's names 	need of care is a child.		
Foreign Birth Certificate (certified translation required if birth certificate not in English or French) Personal information elements required (<i>all other elements redacted</i>): <ul style="list-style-type: none"> • Name • Date of birth • Parent's name(s) 	Foreign Birth Certificate should be provided in the absence of a Long-Form Birth Certificate (e.g., child of permanent resident/immigrant families born in the country of origin). It provides evidence of date of birth, names of the child and of the parent(s), thus confirming need for care for the "child care" category. <u>Parent's Name(s)</u> : to cross-reference with information provided in LMIA application/TFW System. Parent's name(s) on Birth Certificate must be same as Employer's name(s). <u>Child's name and date of birth</u> : will provide evidence that the individual(s) in need of care is a child.	ESDC	CBSA
Adoption Certificate of Child Personal information elements required (<i>all other elements redacted</i>): <ul style="list-style-type: none"> • Name • Date of birth • Adoptive parent's name(s) • Proof of Guardianship 	Adoption Certificate of Child provides evidence of date of birth, names of the child and of the adoptive parent(s), thus confirming need for care for the "child care" category. Alternative document to confirm need for child care in absence of a Long Form birth certificate. <u>Parent's Name(s)</u> : to cross-reference with information provided in LMIA application/TFW System. Parent's name(s) on the Adoption Certificate must be same as Employer's name(s). <u>Child's name and date of birth</u> : will provide evidence that the individual in need of care is a child.	ESDC	CBSA
CRA Notice of Assessment Personal information elements required (<i>all other elements redacted</i>): <ul style="list-style-type: none"> • name of employer • address of employer 	Notice of Assessment provides evidence of the financial ability to pay the caregiver's wage.	ESDC	CBSA

Table 3: Personal Information Disclosed by ESDC to the CBSA

Data Elements	Reason for which data element is collected, used and/or disclosed	From:	To:
<ul style="list-style-type: none"> line 150 - Total income of employer 			
Specific Genuineness Documents for High and Low Wage LMIAs			
Business Licence Personal information elements required (<i>all other elements redacted</i>): <ul style="list-style-type: none"> Employer/business name Employer address Description of business activities permitted pursuant to business license 	This document, when required, is the best tool to assist officers in assessing whether the employer is actively engaged in the business in respect of which the offer is made and is not always required to support the LMIA application. The notable exceptions are new employers to the program, or employers that have risk factors, such as credible media complaints or past Labour Market Opinion (LMIA) refusals for genuineness and employer compliance reviews (ECRs). A typical business licence will identify an employer's business location, the type of activities that are authorized and will corroborate that an employer is actively engaged in the business with respect of which the job offer has been made. Rationale for required data points: <u>Employer name, address and business activities</u> – to cross reference with information provided on the application / in the system, and available in the public domain in order to substantiate consistency in the active engagement of their business.	ESDC	CBSA
T2 Schedule 125 Income Statement Information Personal information elements required (<i>all other elements redacted</i>):	The T2-125 schedule will provide evidence that the employer generates revenue and is therefore actively engaged in providing goods and/or services in Canada. This CRA information is only requested in circumstances where an officer needs to verify the genuineness of an employer's job offer due to risk factors, including credible media reports or past LMIA refusals for	ESDC	CBSA

Table 3: Personal Information Disclosed by ESDC to the CBSA

Data Elements	Reason for which data element is collected, used and/or disclosed	From:	To:
<ul style="list-style-type: none"> Name of corporation (business name) CRA business number Tax year-end Operating name Description of the operations Business income and expense information Employer Address 	<p>genuineness.</p> <p>Rationale for required data points: <u>Employer business number, name, description and address</u> – to cross reference with information provided on the application / in the system, to substantiate consistency in the active engagement of their business. <u>Business income, tax year end and expense information</u> – evidence that the employer generates revenue by providing goods and/or services and therefore can be used to satisfy the officer that the employer is actively engaged in their business.</p>		
<p>T2 Schedule 100 Balance Sheet Information</p> <p>Personal information elements required (<i>all other elements redacted</i>):</p> <ul style="list-style-type: none"> Name of corporation (business name) CRA business number Tax year-end Net income (assets, liabilities, shareholder equity and retained earnings) Employer Address 	<p>This T2 – schedule 100 balance will provide evidence that the employer generates revenue and is therefore actively engaged in providing goods and/or services in Canada.</p> <p>The CRA information is only requested in circumstances where an officer needs to verify the genuineness of an employer's job offer due to risk factors, including credible media reports or past LMIA refusals for genuineness and ECRs.</p> <p>Rationale for required data points: <u>Employer name and address</u> – to cross reference with information provided on the application / in the system, to substantiate consistency in the active engagement of their business.</p> <p><u>Financial information (net income and tax year end)</u> – evidence that the employer generates revenue by providing goods and/or services and therefore can be used to satisfy the officer that the employer is actively</p>	ESDC	CBSA

Table 3: Personal Information Disclosed by ESDC to the CBSA

Data Elements	Reason for which data element is collected, used and/or disclosed	From:	To:
	engaged in their business.		
Workers' Compensation Clearance Letter	The worker's compensation clearance letter will corroborate that an employer is reasonably able to fulfill the working conditions that are consistent with Canadian standards and the terms outlined in the LMIA.	ESDC	CBSA
WRAPA Certificate (Manitoba) <ul style="list-style-type: none"> Employer tombstone information 3rd party information 	The WRAPA Certificate will corroborate that an employer (or recruiter if registration with province is required) is in good standing with respect to employment (or recruitment) legislation in the Manitoba.	ESDC	CBSA
Annex to the appointment of representative form (ESDC EMP 5520) Personal information elements required (<i>all other elements redacted</i>): <ul style="list-style-type: none"> Surname Given name(s) Business name Signature of the employer Name of representative Signature of the representative 	<p>All third parties charging a fee for support with the LMIA application process must be authorized and be one of the following:</p> <ul style="list-style-type: none"> lawyers and paralegals who are members in good standing of a Canadian provincial or territorial law society Notaries who are members in good standing of the Chambre des notaires du Québec, and Immigration consultants who are members in good standing of the Immigration Consultants of Canada Regulatory Council <p>Rationale for required data points: <u>Business name, employer signature and name of representative</u> The elements on the form confirm whether the 3rd party representative is authorized and if the employer has consented to being represented by that third party.</p>	ESDC	CBSA
T2 Schedule 125 Income Statement Information Personal information elements required (<i>all other elements</i>	<p>The T2-125 schedule will provide evidence that the employer generates revenue and is therefore actively engaged in providing goods and/or services in Canada.</p> <p>This CRA information is only requested in circumstances where an officer</p>	ESDC	CBSA

Table 3: Personal Information Disclosed by ESDC to the CBSA

Data Elements	Reason for which data element is collected, used and/or disclosed	From:	To:
<i>redacted</i>): <ul style="list-style-type: none"> Name of corporation (business name) CRA business number Tax year-end Operating name Description of the operations Business income and expense information Employer Address 	<p>needs to verify the genuineness of an employer's job offer due to risk factors, including credible media reports or past LMIA refusals for genuineness.</p> <p>Rationale for required data points: <u>Employer business number, name, description and address</u> – to cross reference with information provided on the application / in the system, to substantiate consistency in the active engagement of their business. <u>Business income, tax year end and expense information</u> – evidence that the employer generates revenue by providing goods and/or services and therefore can be used to satisfy the officer that the employer is actively engaged in their business.</p>		
Federal Skilled Worker Program			
T2 schedule 100 and 125 Personal information elements required (<i>all other elements redacted</i>): <ul style="list-style-type: none"> name of employer, BN # of employer, Schedule 100 line 3849 Retained earnings Schedule 125 line 9999 Net Income - Total income of employer (that will allow an Officer to determine financial ability to pay .	<p>The T2 schedules are collected each time new employers and returning employers as they are usually returning in a different tax year).</p> <p>The T2 schedules 100 and 125 will allow an Officer to determine financial ability to pay the wage).</p>	ESDC	CBSA
CRA PD7A	FSWP has a requirement that employers must be in operation for minimum	ESDC	CBSA

Table 3: Personal Information Disclosed by ESDC to the CBSA

Data Elements	Reason for which data element is collected, used and/or disclosed	From:	To:
Personal information elements required (all other elements redacted): <ul style="list-style-type: none"> • Business number • Employer name • Number of employees in last pay period End of remitting period for which deductions were withheld.	<p>1 year. The CRA PD7A is used as evidence that the business is operating until they submit their next annual tax. Also, to make sure the employment is not seasonal.</p> <p>The business number, employer name and address are cross referenced with the information submitted on the LMIA application – to verify the information pertains to the same employer.</p> <p>The number of employees on the last pay period is to provide proof that the employer is paying employees.</p>		
CRA T4 Summary of Remuneration Paid Personal information elements required (all other elements redacted): <ul style="list-style-type: none"> • Employer Account Number • Employer Name and Address • Total Number of T4 Slips 	<p>The T4 summary will provide evidence that the employer generates revenue and is therefore actively engaged in providing goods and/or services in Canada.</p> <p>Rationale for required data points: <u>Employer name and address</u> – to cross reference with information provided on the application / in the system, to substantiate consistency in the active engagement of their business.</p> <p><u>Financial information</u> – evidence that the employer generates revenue for the purpose of substantiating that they are actively engaged. Provides an officer with an overview of number of employees and the total wages paid in said tax year, again we look at seasonal and/or part time positions.</p>	ESDC	CBSA
T2125 Personal information elements required (all other elements redacted): <ul style="list-style-type: none"> • Name of corporation 	<p>The T2125 will provide evidence that the employer generates revenue and is therefore actively engaged in providing goods and/or services in Canada.</p> <p>This CRA information is only requested for Sole proprietorship in lieu of T2 schedule 100 and 125 in circumstances where an officer needs to verify the</p>	ESDC	CBSA

Table 3: Personal Information Disclosed by ESDC to the CBSA

Data Elements	Reason for which data element is collected, used and/or disclosed	From:	To:
(business name) . <ul style="list-style-type: none"> • CRA business number • Fiscal Period • Operating name • Description of the operations • Business income and expense information • Employer Address • Product or Service • Industry Code 	genuineness of an employer's job offer due to risk factors, including credible media reports or past LMIA refusals for genuineness. Rationale for required data points: <u>Employer business number, name, description and address</u> – to cross reference with information provided on the application / in the system, to substantiate consistency in the active engagement of their business. <u>Business income, tax year end and expense information</u> – evidence that the employer generates revenue by providing goods and/or services and therefore can be used to satisfy the officer that the employer is actively engaged in their business.		
Transition Plan			
Payroll statements Personal information elements required (<i>all other elements redacted</i>): <i>TFWs and Canadian/permanent residents</i> <ul style="list-style-type: none"> • employee name • employee number • wage • deductions • hours of work • hourly wage • benefits • first three numbers of the 	For ESDC to determine if an employer followed through on their commitments through the transition plan requirements. The payroll data elements are critical in assessing an employer's transition to a Canadian and/ PR workforce (evident with the first three numbers of a SIN). It is also used for the assessment of whether or not the employer followed through on commitments to increase wages, provide additional benefits and offer flexible hours.	ESDC	CBSA

Table 3: Personal Information Disclosed by ESDC to the CBSA

Data Elements	Reason for which data element is collected, used and/or disclosed	From:	To:
SIN if applicable			
Timesheets Personal information elements required (all other elements redacted): <ul style="list-style-type: none"> • employee name • employee number • hours of work 	Timesheets are used in combination with payroll statements to determine whether the employer followed through on commitments to offer flexible hours.	ESDC	CBSA
Travel itinerary/Invoices Personal information elements required (all other elements redacted): <ul style="list-style-type: none"> • traveller's name • point of origin • destination • travel date • copy/proof of payment of transportation costs 	For ESDC to determine if an employer followed through on commitments to relocated Canadians/PRs for employment. The travel itinerary/invoices assist in substantiating that the employer paid for transportation. *submitted with a signed letter of consent from the individual to whom the travel itinerary/invoice belong.	ESDC	CBSA
Invoices (ongoing advertising, participation at job fairs) Personal information elements required (all other elements redacted): <ul style="list-style-type: none"> • authorized purchasers name • copy/proof of payment of 	For ESDC to verify start and end date of advertisement to ensure that employers have followed through advertising commitments and to verify that the employer attended a job fair (in particular, where the employer committed to attending multiple job fairs) *submitted with a signed letter of consent from the individual to whom the invoices belong.	ESDC	CBSA

Table 3: Personal Information Disclosed by ESDC to the CBSA

Data Elements	Reason for which data element is collected, used and/or disclosed	From:	To:
<ul style="list-style-type: none"> • dates 			
<p>Employment Contract/Letter of Offer</p> <p>Personal information elements required (<i>all other elements redacted</i>):</p> <ul style="list-style-type: none"> • employer contact information: business name, surname and given name, address, phone number, fax number and email address • employee contact information: surname and given name, home address, phone number, fax number and email address • duration of contract • job description • work schedule (hours) • wages and deductions • bursaries/scholarships • relocation costs • training opportunities 	<p>For ESDC to verify that the employer followed through on their commitments to transition to Canadian/PR workforce and their commitment to providing any of the following as incentives:</p> <ul style="list-style-type: none"> • increase wages offered • part-time or other flex-time/shift work options • bursaries/scholarships • financial support for relocation • training programs <p>*submitted with a signed letter of consent from the individual to whom the employment contract or letter of offer belong.</p>	ESDC	CBSA
Employer Compliance			
Employer Compliance Review (ECR) Results:	For the purpose of the CBSA investigating any other alleged non-compliance with the IRPA	ESDC	CBSA

Table 3: Personal Information Disclosed by ESDC to the CBSA

Data Elements	Reason for which data element is collected, used and/or disclosed	From:	To:
Wages, Occupation and Working Conditions (WOW) of the LMIA confirmation <ul style="list-style-type: none"> • employer name • contact information • job title, occupation and NOC codes • results of findings, including areas of non-compliance and associated corrective actions to be undertaken • findings of non-compliance • ECR period 			
Inspection Results: Conditions of the LMIA confirmation <ul style="list-style-type: none"> • employer name and contact information • job title, occupation and NOC codes • results of findings, including areas of non-compliance and associated corrective 	For the purpose of the CBSA investigating any other alleged non-compliance with the IRPA	ESDC	CBSA

Table 3: Personal Information Disclosed by ESDC to the CBSA

Data Elements	Reason for which data element is collected, used and/or disclosed	From:	To:
actions to be undertaken <ul style="list-style-type: none"> findings of non-compliance inspection or review period 			
Ministerial Instructions: <ul style="list-style-type: none"> employer name and contact information job title, occupation and NOC codes type of instruction ordered date of decision 	For the purpose of the CBSA investigating any other alleged non-compliance with the IRPA	ESDC	CBSA

Upon request, or on its own initiative, as appropriate, the CBSA may disclose the following information to ESDC for the purposes of assessing requests for LMIAs, reviewing such opinions or carrying out an inspection under the IRPR:

- information related to employers who have submitted an application under the TFWP/FSWP and for which charges have been laid as well as when convictions are rendered
- aggregate and non-case specific statistical information on TFWP-related criminal investigations
- additional information as may be requested by ESDC and for which the CBSA has the authority to disclose under the *Privacy Act*, but excluding the disclosure of case-specific information pertaining to ongoing criminal investigations
- convictions under the IRPA of employers who requested or received an LMIA

- information received by the CBSA, including tips from third parties, that may not warrant criminal investigation and would instead be more appropriately addressed through regulatory actions by ESDC

Furthermore, the CBSA will endeavour to inform ESDC prior to undertaking public communications activities related to a TFWP-related criminal investigation. Table 4 reflects the criminal charges/convictions information which will be shared with ESDC:

Table 4: Criminal Charges/Conviction Information Disclosed by the CBSA to ESDC

Data Elements	Reason for which data element is collected, used and/or disclosed	From:	To:
Surname (of Subject)	To help assess requests for LMIAs, review such opinions or carry out an inspection under the IRPR	CBSA	ESDC
Given name(s) (of Subject)	To help assess requests for LMIAs, review such opinions or carry out an inspection under the IRPR	CBSA	ESDC
Country of Residence (of Subject)	To help assess requests for LMIAs, review such opinions or carry out an inspection under the IRPR	CBSA	ESDC
Date of Birth (of Subject)	To help assess requests for LMIAs, review such opinions or carry out an inspection under the IRPR	CBSA	ESDC
Address (of Subject)	To help assess requests for LMIAs, review such opinions or carry out an inspection under the IRPR	CBSA	ESDC
Business Number (if applicable)	To help assess requests for LMIAs, review such opinions or carry out an inspection under the IRPR	CBSA	ESDC
Business Name (if applicable)	To help assess requests for LMIAs, review such opinions or carry out an inspection under the IRPR	CBSA	ESDC
Operating Name(s) (if applicable)	To help assess requests for LMIAs, review such opinions or carry out an inspection under the IRPR	CBSA	ESDC
Case Number	To help assess requests for LMIAs, review such opinions or carry out an inspection under the IRPR	CBSA	ESDC
Criminal Investigations Office	To help assess requests for LMIAs, review such opinions or carry out an inspection under the IRPR	CBSA	ESDC
Date Charges Laid	To help assess requests for LMIAs, review such opinions or carry out an inspection under the IRPR	CBSA	ESDC

Table 4: Criminal Charges/Conviction Information Disclosed by the CBSA to ESDC

Data Elements	Reason for which data element is collected, used and/or disclosed	From:	To:
	inspection under the IRPR		
Date Prosecution Concluded	To help assess requests for LMIAs, review such opinions or carry out an inspection under the IRPR	CBSA	ESDC
Act/Section under which charges were laid	To help assess requests for LMIAs, review such opinions or carry out an inspection under the IRPR	CBSA	ESDC
Prosecution Results	To help assess requests for LMIAs, review such opinions or carry out an inspection under the IRPR	CBSA	ESDC
Sentence(s)	To help assess requests for LMIAs, review such opinions or carry out an inspection under the IRPR	CBSA	ESDC

SECTION 4 - FLOW OF PERSONAL INFORMATION

4.1 Data Flow Model - Diagram

The management, administration and enforcement of the TFWP and FSWP are complex and the processes for collection, use and disclosure of personal information differ across the government departments and agencies. For the CBSA, the following four areas utilize TFWP/FSWP personal information:

Border Services Officers (BSOs): BSOs gather information from a variety of sources to determine the eligibility and admissibility of the FN, including the WP application, Letter of Introduction, GCMS-FWS interface, other information systems, and directly from the FN at the POE.

Criminal Investigators (CIs): Investigators working in the Regional Criminal Investigations Units (CIU) and headquarters Criminal Investigations Program (CIP) of the CBSA receive information from ESDC and CIC (and other sources) regarding potential unlawful activity of employers and/or FNs within the TFWP/FSWP. Information received from ESDC for TFWP/FSWP investigations may include personal information of FNs, employees of the company, and other personal information.

Inland Enforcement Officers/Intelligence Analysts (IAs): Officers of the Inland Enforcement Operations Division (IEOD) are responsible for investigating cases and presenting evidence before the IRB, which may lead to the detention and/or removal of the FN. For the TFWP, the most common investigations are of individuals who are not working at the location where the WP mandates, FNs remaining in Canada past the time permitted on WP, and other similar allegations related to the TFW.

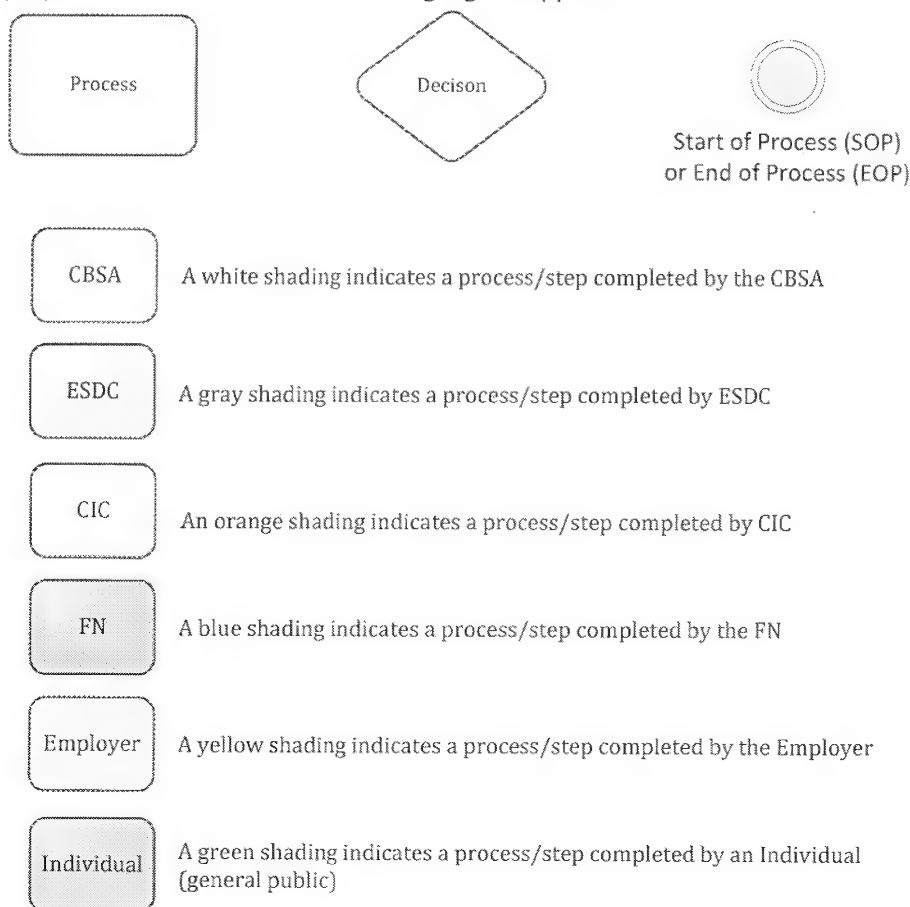
Intelligence Officers (IOs): The Intelligence Operations and Analysis Directorate (IOAD), and regional intelligence units, provide intelligence support to the CBSA and partner operations. They collect information for use by pertinent staff; most notably BSOs and investigators from CIP and IEOD.

All four of the above groups may request and use ESDC information. In terms of disclosure of information to ESDC, CIP and Regional Criminal Investigations Unit staff are the most likely to share information. To a lesser extent, IEOD may provide information to ESDC, but it will be in very limited instances.

BSOs are highly unlikely to disclose information to ESDC as they are interested in receiving information from ESDC to support the examination of FNs at the border. Any information BSOs obtained that could be shared with ESDC would likely be shared by the CIP, Regional Criminal Investigations Unit or IEOD.

IOAD and regional intelligence units may disclose information to ESDC but it is unlikely as IOAD and regional intelligence disclosures are almost entirely to CBSA enforcement programs and various Joint Task Forces.

For the purposes of this section the following legend applies:



The work flows described in this section are as follows:

1. Determine Eligibility and Admissibility of FW at POE
2. Request and Receive Tip Line Information (ESDC Disclosure to CBSA)
3. Receipt of Information After an Employer Compliance Review and/or Inspection
4. Public Interest Disclosure

In addition to these work flows, the CIP, Regional CIU, IEOD and IOAD may request case-specific information in accordance with the ISA. These requests are handled by ESDC on a case-by-case basis, will be assessed in the same manner as described in Section 4.3, and will be shared (if applicable) \

4.2 Determine Eligibility and Admissibility of FW at POE

As reflected in Section A of the Introduction to this PIA, a prospective FN worker may be required to obtain an LMIA and/or a WP, and a visa depending on various factors. This section provides the work flow that employers must follow when seeking to hire a FN to work in Canada.

The work flow described below is supported by Figures 2 and 3 which reflect visual depictions of the various requirements and the work flow. Figure 2 provides a swim lane diagram reflective of the possible requirements for a FN to work in Canada. Figure 3 reflects a work flow under the assumption that the FN requires a WP, an LMIA, and a visa.

The description below follows the work flow provided in Figure 3.

Step 1.0: Complete LMIA Application (Employer)

In this step, the employer completes the appropriate LMIA Application and submits it to ESDC. The type of application completed by the employer varies based on the type of work to be performed. The various types and links to the related forms are found below, while the application for higher-skilled workers is also attached to this PIA as Annex D:

- **High-wage and Low-wage Positions (also attached to this PIA as Annex D):**
[http://www.servicecanada.gc.ca/eforms/forms/esdc-emp5602\(2015-03-001\)e.pdf](http://www.servicecanada.gc.ca/eforms/forms/esdc-emp5602(2015-03-001)e.pdf)
- **In-Home Caregiving Occupations:**
[http://www.servicecanada.gc.ca/eforms/forms/esdc-emp5601\(2015-02-002\)e.pdf](http://www.servicecanada.gc.ca/eforms/forms/esdc-emp5601(2015-02-002)e.pdf)
- **Seasonal Agricultural Worker Program:**
[http://www.servicecanada.gc.ca/eforms/forms/esdc-emp5389\(2014-08-014\)e.pdf](http://www.servicecanada.gc.ca/eforms/forms/esdc-emp5389(2014-08-014)e.pdf)
- **Federal Skilled Worker and Trades Programs:**
[http://www.servicecanada.gc.ca/eforms/forms/esdc-emp5593\(2015-04-005\)e.pdf](http://www.servicecanada.gc.ca/eforms/forms/esdc-emp5593(2015-04-005)e.pdf)

Once the application is completed, the employer submits it to ESDC for consideration and Step 2.0 is triggered.

Step 2.0: Assess LMIA Application (ESDC)

Step 3.0: Provide LMIA to Employer (ESDC)

In Step 2.0, the LMIA application is reviewed by ESDC against the relevant sections of IRPR (section 82, 203 and 209). The LMIA is used to determine whether the employment of a FN is likely to have a positive or negative effect on the Canadian labour market. In Step 3.0, the employer is informed of ESDC's opinion regarding the LMIA. If the LMIA supports the FN working in Canada, the employer is notified and Step 4.0 is triggered.

Step 4.0: Provide LMIA Confirmation Letter to FN (Employer)

In Step 4.0, the employer provides the FN with the annex to the LMIA Confirmation Letter, which the FN provides to CBSA at the POE. However, failing to have this copy will not result in a negative admissibility decision; employers sometimes forget to provide the letter to the FN.

In the assumed scenario for this work flow, once the LMIA Confirmation Letter annex is provided to the FN, the FN may apply for his/her visa and WP. These steps are done in parallel. For the purposes of Figure 3, Steps 5.0 and 8.0 are done simultaneously, as are CIC's assessments at Steps 6.0 and 9.0.

Step 5.0: Apply for Work Permit (FN)

In this step, the FN completes the WP Application, as well as any accompanying forms, and submits them to CIC for an assessment. The WP application form is attached to this PIA as Annex F, but can also be found at the following hyperlink:

<http://www.cic.gc.ca/english/pdf/kits/forms/IMM1295E.pdf>

Other related forms are found here:

<http://www.cic.gc.ca/english/information/applications/work.asp>

Once submitted to CIC, Step 6.0 is triggered.

Step 6.0: Assess WP Application (CIC)

Step 7.0: Issue "Letter of Introduction" (CIC)

In Step 6.0, the WP Application, and any accompanying forms or documents, are reviewed and assessed by CIC. If the WP Application is approved, the FN is provided a "Letter of Introduction" (Step 7.0). As stated earlier in this PIA, the letter is not the WP. The official WP document is only issued by CBSA at the POE after the FN has been determined eligible to work in Canada and the CBSA has determined the FN to be admissible to enter Canada.

Once the Letter of Introduction is provided to the FN, Step 8.0 is triggered.

Step 8.0: Apply for Temporary Resident Visa-TRV (FN)

In this step, the FN completes the Temporary Resident Visa (TRV) application, any accompanying forms, and submits them to CIC for an assessment. The TRV application form can be found here and is also attached to this PIA as Annex G:

http://www.cic.gc.ca/english/pdf/kits/forms/IMM5257B_1.pdf

Other related forms are found here:

<http://www.cic.gc.ca/english/information/applications/work.asp>

Once submitted to CIC, Step 9.0 is triggered.

Step 9.0: Assess TRV Application (CIC)

Step 10.0: Issue TRV (CIC)

Step 11.0: Travel to Canada (FN)

Step 12.0: Assess FN for admissibility, including TFW requirements (CBSA)

In Step 9.0, the TRV Application, and any accompanying forms or documents, are reviewed and assessed by CIC. If the TRV Application is approved, the visa, which is an official counterfoil document issued by a CIC visa office abroad, is placed in the FN's passport to show that he or she has met the requirements for admission to Canada as a temporary resident (Step 10.0).

In the scenario presented in this work flow, once the FN has his/her "Letter of Introduction" (Step 7.0) and TRV (Step 10.0), he or she is ready for travel to Canada (Step 11.0).

At Step 12.0, upon arriving at a POE, the FN is assessed by the CBSA for admissibility to enter Canada and for eligibility to work in Canada. To determine eligibility under the TFWP, the BSO will access GCMS (FOSS in some areas until FOSS is decommissioned) which will allow view only access to ESDC's FWS data. The type of personal information the BSO is permitted to view is limited to the LMIA Application and resulting decisions by ESDC (see Steps 1.0 and 2.0).

If the BSO is satisfied that the FN meets the eligibility and admissibility criteria, a WP is issued and the FN is permitted entry to Canada. If there are issues regarding customs seizures or admissibility issues, data may be entered into the ICES.

Note: For visa-exempt foreign nationals, the CBSA assesses the WP application at the POE and issues the WP, if eligibility and admissibility criteria are met.

Figure 2: Determine Eligibility and Admissibility of Foreign National for TFWP

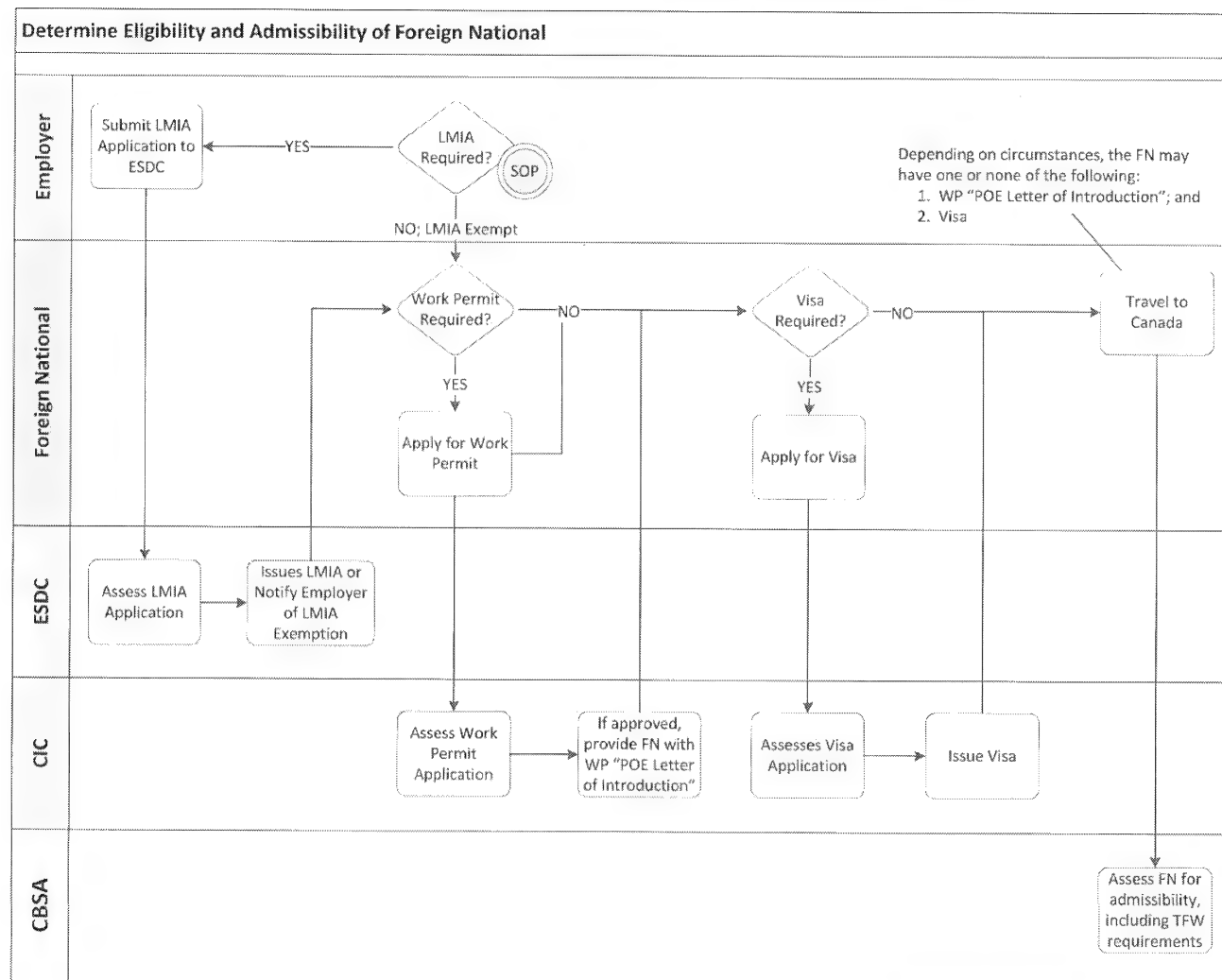
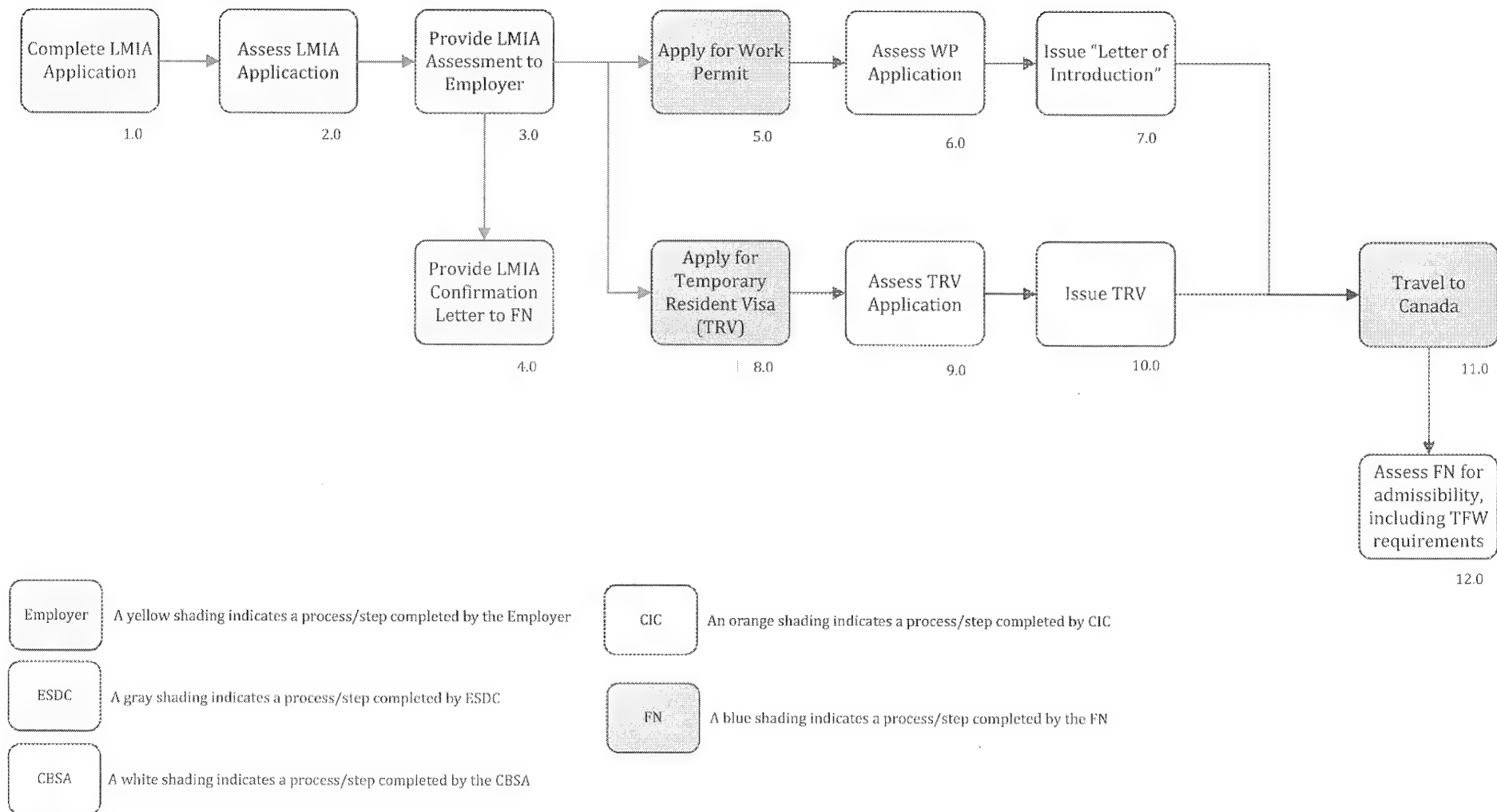


Figure 3: Determine Eligibility and Admissibility of Foreign National at POE for TFWP

4.3 Request and Receive Tip Line Information (ESDC Disclosure to CBSA)

In spring 2014, amidst several cases of alleged mistreatment of FNs and violations of the TFWP by some employers, ESDC sought avenues for FNs and concerned individuals to provide information regarding potential abuse of the TFWP by employers or individuals, to the federal government. Therefore, in summer 2014, an Online Fraud Reporting Tool (OFRT) was established, which allows for an individual to contact ESDC via telephone (voicemail only) or a web form (<http://www.servicecanada.gc.ca/eng/about/integrity/tfwp/reporting.shtml>). The individual is informed on the voicemail and the web form that it is their option to remain anonymous or provide name and contact information.

The OFRT provides proper notice and consent to individuals before they provide information via the online tool. Annex H to this PIA details the information provided to an individual before they submit information via the web form.

The tip information is maintained and tracked by ESDC's Service Canada's Integrity Services Branch (ISB) in an ESDC SharePoint site. The information is not stored in the FWS. The voicemails are listened to and transcribed verbatim into a document that is stored in SharePoint. Web form data is also stored on the SharePoint site and is not edited by ISB.

All tips received by ISB are assessed to determine if they are legitimate. Once ISB establishes the validity of the tip, it will search the FWS for other information to among other things, accurately identify the appropriate FN, third party, or employer. If, after the assessment of the tip, ISB believes the case may warrant an ECR or other action, it will assign the case to the appropriate regional ISB staff.

The overwhelming majority of tips received since summer 2014 have been handled entirely by ESDC; however, a small number of tips involved information that must be investigated for possible enforcement action by the CBSA. The work flow below describes the steps supporting the disclosure of information received via the OFRT to the CBSA.

This section is supported by Figure 4.

Step 1.0: Complete ESDC Online Fraud Reporting Tool (Individual); or Step 1.0: Provide Fraud Tip Via Voice Mail (Individual)

The process begins by an individual providing a tip via the OFRT web form or voicemail. For the OFRT, after being presented with the information found in Annex H of this PIA, the individual is asked to provide consent to use the information they provide. The individual must provide consent by selecting "Yes" or information cannot be submitted via the web form.

Subsequently, the individual is asked if, he/she will be in imminent danger or be at risk of serious physical injury by providing information on the web form. If the person answers "Yes", they are presented with the following Service Canada Confidential Tip Line phone number (1-866-602-9448), and are not permitted to submit information via the web form.

Assuming the individual responds by stating he/she is not in any serious physical danger, the web form is completed with information relating to the suspected or alleged program abuse and/or fraud and the

individuals involved. Finally, the web form provides the individual with an option to provide their contact information. As reflected earlier in the process, anonymity is permitted. However, if the individual wishes to provide his/her information, they are asked to provide the following:

1. First Name
2. Last Name
3. Contact Telephone Number
4. A free text field to provide other contact information details

The web form is sent to an ESDC general delivery mailbox and assessed by the ISB.

For individuals who submit their tip via the telephone number (voicemail only), the voice mail is also managed by ISB. Internal procedures require the voicemail to be monitored daily.

If the information provided by the individual merits a referral to the CBSA for enforcement of the IRPA/IRPR, Step 2.0 is triggered.

Step 2.0: Complete "CBSA Lead Referral from SC/ISB" Form

In Step 2.0, if there is sufficient information to support a referral to the CBSA for potential enforcement action, ISB staff complete a form called "CBSA Lead Referral from SC/ISB". The form, attached to this PIA as Annex I, is emailed to CBSA CIP and will include all information provided from the tip. The tip will not include any other information from ISB's information systems, FWS, or any other ESDC information system. CBSA receives all information provided by the individual who provided the tip, including the individual's name and contact information, except when anonymity was requested.

Step 3.0: Receive Referral Form and Generate Lead in CIIMS

Step 4.0: Assign to Appropriate Regional Investigator

The email account to which ESDC sends the email is maintained by CIP HQ. Once the form is received by CIP (Step 3.0), and if it contains sufficient information to proceed, it is used to generate a lead in CIIMS and may create an investigation assignment (in CIIMS) to a regional investigator (Step 4.0).

Once the investigation activity is assigned, Step 5.0 is triggered.

Step 5.0: Initiate Investigation

Step 6.0: Request Information from ESDC (if required)

In Step 5.0, the appropriate regional investigator initiates an investigation. The types of activities that are required to perform an investigation vary on a case-by-case basis. However, if during the investigation, a search warrant or prosecution is sought by the regional investigator, he/she will seek paper copies of various data from ESDC; most often a copy of the LMIA and correspondence between ESDC and the employer/individual. In Step 6.0, to obtain those paper copies, the regional investigator will send to the TFWP at ESDC requesting paper copies to support a search warrant or prosecution. The email from the CBSA must include at least the following information:

1. Name of employer, third party or TFW, System File Number and other identifying details to ensure accuracy of the information;
2. The section of the IRPA to which the investigation and the requested ESDC information relates;
3. Timeframe of the records (for example, the CBSA may request all LMIA's provided to an employer over the last three years); and
4. A description of the exact documentation being sought by the CBSA (e.g. copies of the LMIA's, any correspondences, etc.).

Once the email is received by ESDC, Step 7.0 is triggered.

Step 7.0: Assess CBSA Request for Paper Copies

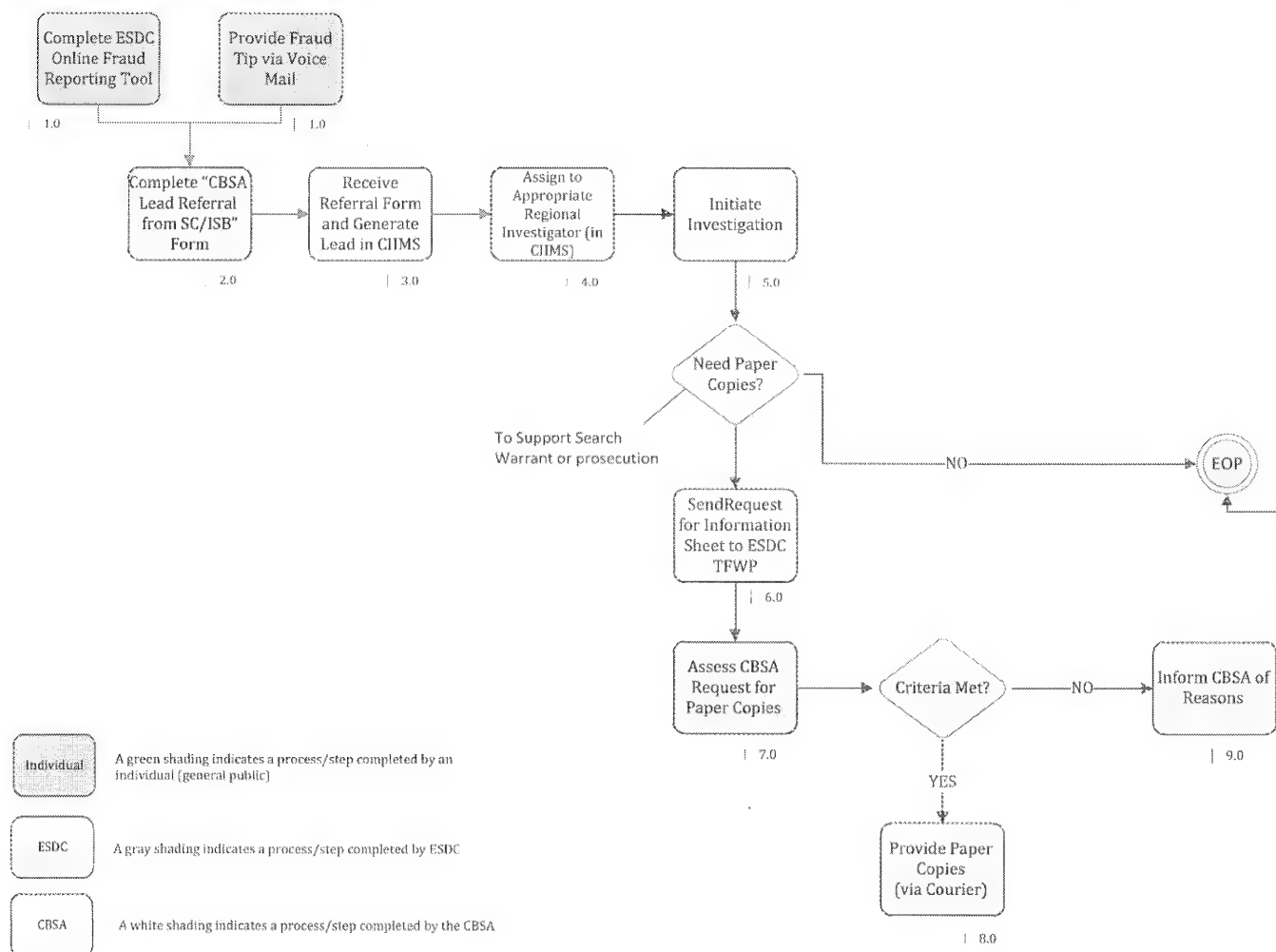
Step 8.0: Provide Paper Copies (via Courier)

In Step 7.0, ESDC assesses the CBSA's request to determine if it can disclose the information under sub-section 34(1) of the DESDA. This assessment allows ESDC to determine if information could be further disclosed under sub-section 35(1) of DESDA. In its assessment, ESDC will analyze the request against the ISA and determine what, if any, information can be released. If the program can disclose information, ESDC provides copies of the information via courier (Step 8.0).

Once provided to the CBSA, the copies are stored in paper files. CIIMS has the ability to mark/identify the ESDC records as a source provided to the CBSA in accordance with the ISA. Furthermore, copies of documents that are provided to the CBSA are identified/marked with the source as being provided via the ISA and subject to secondary disclosure restrictions of the ISA.

The copies are shared with the court (search warrant and prosecution), the Public Prosecution Service of Canada (PPSC) and the Defence attorney. The court could be federal, provincial or territorial. If the investigation is part of a joint investigation, the CBSA may share the information obtained during the execution of the search warrant with the partner agency; e.g. RCMP.

Step 9.0: Inform CBSA of Reasons (ESDC)

Figure 4: Request and Receive Tip Line Information (ESDC Disclosure to the CBSA CIP)

4.4 Receipt of Information After an Employer Compliance Review and/or Inspection

As part of its responsibilities under the TFWP, ESDC may obtain information during an ECR and/or inspection of an employer which prompts the need to refer particular information to CBSA Regional CIU. This type of disclosure is performed regionally and varies as to whether the information is delivered via email or courier. These types of disclosures are anticipated to be done via courier, and again, are only provided to CBSA when it meets the disclosure provisions of the DESDA/DESDR and in relation to the administration and enforcement of the IRPA/IRPR.

4.5 Public Interest Disclosure

In addition to the above, ESDC may, on its own initiative, release information to the CBSA for IRPA/IRPR enforcement purposes if the TFWP is aware of specifics that would warrant invoking the Minister's authority under sub-section 37(1) of the DESDA. Sub-section 37(1) allows ESDC to disclose information if, in the Minister's opinion, the public interest clearly outweighs any invasion of privacy that could result from the disclosure. If ESDC makes any disclosure pursuant to sub-section 37(1) of the DESDA, it is required by sub-section 37(2) to notify the Privacy Commissioner prior to disclosure (if reasonably practicable) and the Privacy Commissioner may choose to notify the individual whose information is being disclosed.

4.6 Data Flow Model - Table

This table summarizes the flow of data illustrated in the data flow diagram above. From whom or from what organization is the personal information collected? In other words, identify who is providing the personal information that is being used, will be used, or available for use for the program or activity. For multiple sources, indicate all sources.

SOURCE	IDENTIFY THE SOURCE
The individual or a representative	Individual (Foreign Worker) Individual (Providing abuse fraud information; if they chose not to remain anonymous) Employer (if a sole proprietor; and contact person for the corporation, which is provided on the LMIA Application – See Annex D) Individual (3 rd Party Representative – See Annex E)
A federal government institution (identify from what PIB the information is obtained)	CIC (CIC PPU 039, International Service: Overseas Immigration Case Files; and CIC PPU 054, Temporary Worker Records and Case File) ESDC (CIC PPU 440, Temporary Foreign Worker Program, ESDC PPU 171, National Integrity Investigation for EI ⁴) CBSA (TFWP, CBSA PPU 050, CBSA PPU 035, CBSA PPU 1402)
Non federal institutions	
- Provincial Government	N/A
- Municipal Government	N/A
- Aboriginal Government / Council	N/A
- Organization of a Foreign State	N/A
- International Organization	N/A
Private Sector	
- Located in Canada and Canadian Owned	N/A
- Located in Canada and Foreign Owned	N/A
- Located abroad and Canadian Owned	N/A
- Located abroad and Foreign Owned	N/A

4.7 Internal Use and Disclosure

Where will the information circulate within the CBSA? Identify any related programs or activities and personal information banks as identified in the CBSA Info Source chapter.

⁴ ESDC PPU 171, along with PPU 440, are identified in LMIA applications, but ESDDC PPU 171 requires an update to align it with the TFWP. ESDC has identified this in their PIA.

Program

Operations/Intelligence (IOAD) and regional intelligence units/criminal investigations (CIP)/ regional criminal investigations unit (CIU)/ Inland Enforcement (IEOD)

Personal information bank

Temporary Foreign Worker Program/CBSA PPU 050, CBSA PPU 035, CBSA PPU 1402)

4.8 External Use and Disclosure

Where will the information circulate outside the CBSA? This includes any disclosure made to:

The individual or a representative

Defence Attorney

A federal government institution

Public Prosecution Service of Canada

(for investigations that result in prosecution)

Immigration and Refugee Board of Canada (IRB): Immigration Division Case Files, IRB PPU 140

Non-federal institutions and private sector

- Provincial/Territorial Government
- Municipal Government
- Aboriginal Government / Council
- Organization of a Foreign State
- International Organization

Courts: For application of search warrant, production order, or prosecution.

Courts: For application of search warrant, production order, or prosecution.

N/A

N/A

N/A

Private Sector

- Located in Canada and Canadian Owned
- Located in Canada and Foreign Owned
- Located abroad and Canadian Owned
- Located abroad and Foreign Owned

N/A

N/A

N/A

N/A

4.9 Retention / Storage

Where will the information be stored or retained? Identify all organizations that will store the information. This includes duplicates of the databases containing the personal information or any back-ups.

The individual or a representative

Defence Attorney

A federal government institution

CBSA: GCMS/FOSS, NCMS, IMS, CIIMS, ICES, STS, Paper files

Public Prosecution Service of Canada

Immigration and Refugee Board of Canada (IRB): Immigration Division Case Files, IRB PPU 140

A Federal Records Centre

N/A

Non federal institutions and private sector

- | | |
|-----------------------------------|--|
| - Provincial Government | Courts: For search warrants, production order, or prosecution. |
| - Municipal Government | Courts: For search warrant, production order, or prosecution. |
| - Aboriginal Government / Council | N/A |
| - Organization of a Foreign State | N/A |
| - International Organization | N/A |

Private Sector

- | | |
|--|-----|
| - Located in Canada and Canadian Owned | N/A |
| - Located in Canada and Foreign Owned | N/A |
| - Located abroad and Canadian Owned | N/A |
| - Located abroad and Foreign Owned | N/A |

4.10 Other Possible Considerations

Identify the areas, groups and individuals who access and handle the personal information:

Identify the areas / groups / divisions who are allowed to access and handle the personal information collected for the program or activity. Also, identify where these areas or groups are located (i.e. national capital region, within a province, in a foreign country, or several locations if tele-working) as well as the location of the personal information to uncover any potential trans-border or inter-jurisdictional issues. Where reasonable to do so, by virtue of the size of the organization or the number of individuals, identify individual positions rather than the work area or group.

The CBSA responsible for program or activity:

Identify Groups or Areas / or Divisions	Positions who have access or use the personal information (where appropriate)	Geographical Location
Border Services Officers	BSOs	Across Canada
IOAD	Intelligence Officers, Intelligence Analysts	Across Canada
Regional Intelligence Units	Junior and Senior Program Officers	Across Canada
	Senior Program Advisors	
CIU	Criminal Investigations Units	Regional - Across Canada
CIP	Criminal Investigators	Headquarters
IEOD	Enforcement Officers	Across Canada
Other federal government Institution responsible for program or activity: (one table per institution):		
CIC	TFWP Staff	Across Canada
ESDC	TFWP Staff/Integrity Services Branch	Across Canada

Canada Border Services Agency

	(ISB) Investigators	
Public Prosecution Service of Canada	Prosecutorial staff	Across Canada
IRB	Court Staff Support Staff	Across Staff
Courts (for search warrant applications and prosecutions)	Judges and their staff	Across Canada
Non Federal Institution or Defence Attorney: 'name': (one table per institution)		
Provincial and Territorial Courts (for search warrant applications and prosecutions)	Judges and their staff	Across Canada

SECTION 5 - PRIVACY COMPLIANCE ANALYSIS

1. Legal Authority For Collection Of Personal Information (if unsure, consult with Legal Services)

Has a legal authority been identified for the collection of personal information for this program or activity?

Statutory reference: Section 4 of *Privacy Act* (Section 4 has been interpreted to mean that a legal authority must be established for a collection of personal information, but section 4 does not provide legal authority for such a collection).

Policy reference: Section 6.2.6 of *Directive on Privacy Practices*

Yes

- 1.1 ☒ Specify the legal authority and briefly explain its connection to the program or activity or how it permits the collection of the personal information:

With respect to the CBSA-ESDC ISA, personal information is collected pursuant to Sections 11, 20 and 22 of the *Immigration and Refugee Protection Act* and Part 11 of the *Immigration and Refugee Protection Regulations*.

In addition to what is identified in the ISA, personal information is also collected by the CBSA under sections 15, 16, and 18 of the IRPA and s. 5 of the *CBSA Act*.

Also, pursuant to paragraph 8(2)(a) of the *Privacy Act*, and under section 209.92 of IRPR, the CBSA has the authority and discretion to disclose information related to the TFWP to ESDC for the administration or enforcement of the TFWP, the FSWP and the IMP.

Also, subsection 4(2) of the IRPA states the Minister of Public Safety and Emergency Preparedness is responsible for administering the Act as it relates to the enforcement of the Act, including arrest, detention and removal.

- 1.2 ☒ Is the personal information collected directly related to an operating program or activity?

Details: TFWP information collected from ESDC, via the ISA, is directly related to the CBSA's responsibility to administer and enforce the IRPA, including the responsibility to issue WPs at POEs, determine the admissibility of persons seeking to enter or remain in Canada, and to investigate and prosecute contraventions of the offence provisions of the IRPA, among others.

→ Continue to Question 2

No

- 1.3 ☐ If there is no legal authority for the collection of personal information, it cannot be collected. Please consult your legal advisor to determine if there is authority to proceed with the program or activity.
****The PIA process must not continue without this key information.****

2. Necessity To Collect Personal Information

Is each element and sub-element of personal information collected or to be collected necessary to administer the program or activity?

Statutory reference: Section 4 of *Privacy Act*

Policy reference: Sections 6.1.1, 6.1.3, 6.1.4, 6.2.7 and 6.2.8 of *Directive on Privacy Practices*

YES

- 2.1 ☒ Ensure that all personal information necessary to administer the program or activity is listed in the relevant **PIB**.

****Personal Information Bank (PIB) should be found within "Section 1 – Overview and Initiation" above****

- 2.2 ☒ AND, implement controls and procedures to ensure the CBSA does not collect more personal information than is necessary for the identified program or activity and that a continuing need exists for that information or its collection.

2.3 Are secondary uses contemplated for the information collected?

****Treasury Board defines a "Secondary Use" as a purpose that is not consistent with the original purpose of the collection.****

☐ YES ☒ NO (Continue to Question 3)

****If you've selected "Yes" to Question 2.3 above, please note that Consent is required for all "Secondary Uses". Please ensure that a "Consent Statement" is created. Please refer to "4. Direct Collection - Notification and Consent (as appropriate)" below for the information required in a "Consent Statement".****

2.3.2 If not, is there authority for the use or disclosure of the personal information?

****Please ensure that the Legal Authority identified above allows for all uses and disclosures of the personal information.****

☐ YES ☐ NO

→ Continue to Question 3

NO

- 2.3 ☐ Review the proposed elements and sub-elements of personal information outlined in "Section 3 – Analysis of Personal Information Elements" to identify those that are "necessary" and not merely useful. Document any changes.

3. Authority For the Collection, Use or Disclosure Of the Social Insurance Number

Is the collection of the Social Insurance Number (SIN) necessary to administer the program or activity?

YES

- 3.1 ☐ Collection of the SIN must be in compliance with the *Directive on Social Insurance Number* (please check all appropriate boxes below):

3.2 ☐ State legal authority for collecting the SIN:

OR, in the absence of a legal authority to collect the SIN:

3.3 ☐ Establish explicit authority through legislative amendment(s).

3.4 ☐ Establish legal authority as outlined in the *Directive on Social Insurance Number*.

AND, if disclosure of the SIN by the CBSA is to occur on a routine or systematic basis

3.4.1 ☐ to another federal institution that is authorized to collect it, or to another level of government, establish an agreement or arrangement that includes specific provisions to limit the use of the SIN.

3.4.2 ☐ to a contractor or other external service provider, establish a contract that includes specific provisions to limit the use of the SIN.

3.5 ☐ AND, ensure that the relevant **PIB** for the program or activity states the authority under which the SIN is collected and the purpose for which it is used.

→ Continue to Question 4

NO

3.6 ☒ The SIN is not necessary and it will not be collected, used or disclosed to administer the program or activity.

→ Continue to Question 4

4. Direct Collection - Notification and Consent (as appropriate)

Is personal information collected directly from the individual to whom it relates?

YES

4.1 ☒ A "Privacy Notice" (adapted for either verbal or written communications) must be provided to the individual at the time of collection and it must include the following elements:

- a) The purpose and authority for the collection
- b) Any uses or disclosures that are consistent with the original purpose.
- c) Any uses or disclosures that are not related to the original purpose

(This element need only be included when additional uses or disclosures on a regular basis are contemplated at the time of collection for a purpose other than the original purpose or a consistent use, in which case a "Consent Statement" may need to be added to the "Privacy Notice" – see below for "Consent Statement" elements.)

- d) Any legal or administrative consequences for refusing to provide the personal information
- e) That the "individual to whom the information relates" has rights of access to, correction of and protection of personal information under the *Privacy Act*.
- f) A reference to the **PIB** for the program or activity

(This element need only be included when the notice is to be given to the individual in writing.)

****For a copy of the CBSA Privacy Notice and Consent Statement template, contact the ATIP Division.****

g) Why the SIN is collected, how it will be used and the consequence of not providing it.

(This element need only be included when the SIN is being collected – refer to “3. Authority For the Collection, Use or Disclosure Of the Social Insurance Number” above.)

AND, add a “**Consent Statement**” to the “**Privacy Notice**” as appropriate, if the personal information is to be used or disclosed for a purpose other than the original purpose (**Secondary Use**) or a consistent use, or, to authorize indirect collection of personal information.

4.2 ☒ The “**Consent Statement**” must include the following elements:

- a) The purpose of the consent and the specific personal information involved.
- b) In the case of indirect collections, the sources that will be asked to provide the information. (This element need only be included when personal information is to be collected from another source e.g., person or organization with the consent of the individual)
- c) Uses and disclosures that are not consistent with the original purpose of the collection and for which consent is being sought.

(This element need only be included when the individual’s consent is sought for a secondary use or disclosure that is not consistent with the original purpose for which the information is collected. To find out if the individual’s consent is necessary for such a use or disclosure, please consult the ATIP Division)

- d) Any consequences that may result from withholding consent.
- e) Any alternatives to providing consent

****For a copy of the CBSA Privacy Notice and Consent Statement template, contact the ATIP Division****

4.3 ☒ AND, implement controls and procedures to ensure that the CBSA keeps a record documenting whether or not an individual provided consent when it was sought, including a record documenting any withdrawal of consent when applicable.

Additional Consent Considerations (s. 77(1)(m) of the *Privacy Act*):

- ☒ Standards and mechanisms are in place to ensure that the individual has capacity to give consent.

→ Continue to Question 5

NO

4.4 ☒ The personal information necessary for the program or activity is not collected directly from the individual. It is collected indirectly, for example, from another program within the CBSA, or from another institution, government or third party.

Note: Information collected as part of the TFWP/FSWP is direct and indirect. For the WP application process, BSOs at the POE obtain information directly from the individual, as well as indirectly from ESDC and CIC. Information on employers (and contact details of employees of the company) as well as third party representative information may be collected at the POE indirectly – from the FN or via the FWS-FOSS/FWS-GCMS interface. However, ESDC and CIC have presented all individuals with a proper Privacy Notice and Consent Statement (when required) to support the CBSA’s use of the information. Also, at the time the FN presents him/herself at the POE, some information may be collected directly from the individual during examination and via the E-311 Form (where applicable). That form is compliant with section 4.1 above.

Also, information collected by the CBSA for investigation and intelligence purposes are not direct collections. They are collected on an as needed basis and used in accordance with the IRPA. Information is collected from ESDC as reflected in Section 4 of this PIA.

→ Continue to Question 5

5. Indirect Collection - Consent or Authority Under Sec. 10 of Privacy Regulations

Is personal information collected indirectly from another source with the informed consent of the individual to whom it relates, or from a person authorized to act on behalf of the individual pursuant to section 10 of the Privacy Regulations?

Statutory reference: Sections 4 and 5 of *Privacy Act* and section 10 of *Privacy Regulations*

Policy reference: Sections 6.1.1, 6.2.6 and 6.2.9 to 6.2.13 of *Directive on Privacy Practices* and sections 6.1.2 and 6.4.1 of the *Directive on Social Insurance Number*

YES

- 5.1 ☒ The notice and consent requirements stated at Question 4 apply. Please provide the "Privacy Notice" and/or "Consent Statement" below:

****For a copy of the CBSA Privacy Notice and Consent Statement template, contact the ATIP Division****

- 5.2 ☒ AND, implement controls and procedures to ensure the CBSA keeps a record documenting whether or not an individual provided consent when it was sought, including a record documenting any withdrawal of consent when applicable.

- 5.3 ☐ AND, if information is being collected from persons authorized to act on behalf of minors, incompetents or individuals who have been deceased for less than 20 years, implement appropriate mechanisms to ensure that such persons are authorized to act on behalf of individuals who do not have the capacity to provide consent.

→ Continue to Question 6

NO

- 5.4 ☐ → Continue to Question 6

6. Indirect Collection - Without Notification and Consent

Is personal information collected from another source without notice to or consent from the individual to whom the information relates?

Statutory reference: Sections 4, 5, 7 and 8 of *Privacy Act* and section 10 of *Privacy Regulations*

Policy reference: Sections 6.2.6 and 6.2.9 to 6.2.13 of *Directive on Privacy Practices*, section 6.2.15 of the *Policy on Privacy Protection* and sections 6.3.2 and 6.3.3 of *Directive on Privacy Impact Assessment*

YES

- 6.1 ☒ Where information is collected indirectly under any of the following circumstances without notice to,

or consent from, the individual to whom it relates, please check the applicable boxes and explain as requested:

- ☒ a) The collection is a result of a disclosure to the CBSA under subsection 8(2) of the *Privacy Act*. State the applicable paragraph(s) of subsection 8(2) and provide a brief explanation for each:

Details: ESDC collects personal information related to the TFW from employers without the explicit consent of the TFW. The TFW provides his/her name to their prospective employer for the purposes of obtaining employment. ESDC is of the view that the provision of personal information by the TFW for consideration of employment is consistent with the employer's disclosure of this information for the same purpose (to ESDC and CIC for the LMIA and WP process). The TFW makes a choice by providing his/her personal information to the employer to determine eligibility for employment. If they did not agree with the employer submitting their information to the TFWP, they would not be considered for eligibility for employment under the program.

- ☒ b) Direct notification of the individual might result in the collection of inaccurate information, or might defeat the purpose or prejudice the use for which the information is collected. Briefly explain why notice is not provided:

- ☐ c) The information involved in the program or activity is to be used solely for a non-administrative purpose in which no decisions are made about the individuals to whom the information relates. (This includes research, statistical, audit or evaluation purposes.)

6.2 ☒ AND, if any of the circumstances in a) b) or c) is applicable, ensure that it is reflected in the relevant **PIB**. Note: this is reflected in the ESDC PIB.

6.3 ☐ AND, if the information is to be used solely for a non-administrative purpose (box c above has been checked), ensure that the requirements under sections 6.3.2 and 6.3.3 of the *Directive on Privacy Impact Assessment* have been met, and that the decision of the official responsible for section 10 of the *Privacy Act* to proceed with a CBSA PIA for the program or activity has been adequately documented in the description of the program or activity in "*Section 1 - Overview and PIA Initiation*" of the CBSA PIA.

6.4 ☐ OR, if none of the circumstances in a) b) or c) is applicable, then the personal information must be collected directly from the individual, or indirectly with the consent of the individual. Please review the responses to Questions 4 and 5 and ensure that the "**Privacy Notice**" or the "**Consent Statement**" includes all of the required elements within Question 4.

→ Continue to Question 7

NO

6.5 ☒ All personal information is collected directly from the individual to whom it relates, or from another source with notice to, or consent from, the individual or a person authorized to act on behalf of the individual (see Questions 4 and 5 above). → Continue to Question 7

7. Retention and Disposal of Personal Information

Has Library and Archives Canada approved a records retention and disposal schedule that applies to the personal information? (Consult Information Management officials to determine the authority to retain and dispose the personal information and provide the relevant details below.)

Statutory reference: Section 12 of *Library and Archives Canada Act*, sections 6, 10 and 11 of *Privacy Act* and section 4 of *Privacy Regulations*

Policy reference: Sections 6.1.3, 6.2.11 to 6.2.13 and 6.2.23 of *Directive on Privacy Practices*

YES

- 7.1 ☒ Please identify the Record Disposition Authority (RDA) and describe the retention and disposal schedule: (For example, RDA Number: 79/002, records are retained for 10 years -- active for five and dormant for five. Destruction through agreement with Library and Archives Canada.)
- 2006/004. Paper records will be retained for 2 years after the last administrative action and then are destroyed. Electronic records are retained indefinitely. Work permits are microfilmed and retained indefinitely at Citizenship and Immigration Canada.
- 7.2 ☒ AND, implement controls and procedures to ensure that personal information used to make a decision that directly affects an individual will be retained for a minimum of two years after the last administrative action or, where a request for access to the information has been received, until such time as the individual has had the opportunity to exercise all his/her rights under the Act.
- 7.3 ☒ AND, if the CBSA intends to dispose of personal information that has been used for an administrative purpose prior to the expiration of the two-year minimum retention standard established by the *Privacy Regulations*, it must obtain the consent of the individual to whom the information relates before doing so.
- 7.4 ☒ AND, the CBSA must cite the RDA number, the retention period and the disposition standards for the personal information in the relevant PIB.
- Continue to Question 8

NO

- 7.5 ☐ Provide a Records Disposition Submission to Library and Archives Canada describing the records containing the personal information for which the institution requires a RDA.
- 7.6 ☐ AND, obtain a RDA from Library and Archives Canada to allow the CBSA, under certain conditions, to dispose of records that no longer have operational utility for the program or activity.
- 7.7 ☐ AND, ensure that all the other applicable requirements listed under "YES" at Question 7 are met.
- Continue to Question 8

8. Accuracy Of Personal Information

Will measures be adopted to ensure that personal information used by the CBSA for an administrative purpose is as accurate, up-to-date and complete as possible?

Statutory reference: Sections 6, 10 and 11 of *Privacy Act* and sections 10 and 11 of *Privacy Regulations*

Policy reference: Sections 6.1.1 and 6.2.9 to 6.2.16 of *Directive on Privacy Practices*

YES

8.1 ☒ Please check any of the following measures that will be adopted to ensure accuracy of the personal information and provide details as requested:

8.1.1 ☒ Personal information will be collected directly from the individual to whom it relates or it will be validated with the individual or a person authorized to act on behalf of the individual.

8.1.2 ☒ A data-matching process will be used to verify the accuracy of personal information against a "reliable source" (within or outside the CBSA) where this is authorized, or where consent was obtained.

is used for ESDC to provide CBSA with information necessary for BSOs, investigators (CIP, regional CIU and IEOD), intelligence officers and intelligence analysts (IOAD and regional intelligence units) to enforce IRPA. The information received from ESDC is data matched against the person(s) or company(ies) who are the subject of an assessment or investigation.

Likewise, the CBSA may upload information for use by ESDC. Upon request, ESDC will request information on a particular company or individual. CBSA will perform a data match to ensure appropriate records are uploaded for ESDC use.

All uploads (by ESDC and CBSA)

Other information sharing will include data matching exercises to ensure the appropriate records are being shared by the CBSA (when CBSA discloses information) and have been received by the CBSA (when CBSA receives information from ESDC).

8.1.3 ☐ In cases where direct collection or consent is not feasible, the CBSA will obtain information from trusted sources (public or private) and verify accuracy against existing personal information before use.

Details: *Identify the sources and procedures to be used to check the accuracy of the information*

8.1.4 ☐ Technological methods will be used to identify errors and discrepancies.

Details: *Describe the technological methods used*

8.1.5 ☐ Other

Specify: *(This information is mandatory)*

8.2 ☐ AND, if measures are adopted other than "direct collection or validation with the individual or with a person authorized to act on behalf of the individual", the CBSA must implement appropriate controls and procedures to ensure that:

a) the technique(s) and the specific source(s) used to validate or update the personal information

are documented;

- b) individuals are given the opportunity, whenever possible, to request correction of any inaccurate personal information before the information is used in a decision-making process that affects them;
- c) personal information can only be modified or corrected by those within the CBSA who have the authority to do so;
- d) when personal information is corrected or annotated, the record of personal information indicates the date of the last correction or annotation and the source of the information used to make the correction or annotation; and
- d) when personal information is corrected or annotated, other authorized holders of the information are notified about the correction or annotation and that all copies of the information in the possession of the CBSA are corrected / annotated.

8.3 ☐ AND, if appropriate, ensure that the "Privacy Notice" or "Consent Statement" and the relevant **PIB** are amended to identify the data-matching activity including the source(s).

→ Continue to Question 9

NO

8.4 ☐

Explain why such measures will not be adopted: *(This information is mandatory)*

→ Continue to next Question 9

9. Use Of Personal Information

Will the personal information collected for the program or activity be used solely for the original purpose for which it was obtained or compiled, a use consistent with that purpose, or a purpose for which the information was disclosed to the institution pursuant to subsection 8(2) of the Privacy Act?

Statutory reference: Sections 5 and 7 to 11 of *Privacy Act*

Policy reference: Sections 6.1.1, 6.1.9, 6.2.9 to 6.2.13 and 6.2.17 of *Directive on Privacy Practices*, section 6.2.15 of *Policy on Privacy Protection* and Section IV of Appendix C of *Directive on Privacy Impact Assessment*

YES

- 9.1 ☒ Implement controls and procedures to ensure that access to the personal information for such purposes will be limited to authorized individuals who need to know the information to perform their official duties. *(Identify the work positions within the program or activity that have a valid reason to access and handle the personal information, and limit access to individuals occupying those positions.)*
- 9.2 ☒ AND, ensure that the "Data Flow Diagram" or "Data Flow Tables" completed for "Section 4 – Flow of Personal Information" of the CBSA PIA identify the areas, groups and individuals (e.g., the positions) within the CBSA who have a need-to-know to access to or handle the personal information, including their geographical location and where the personal information will be stored or retained. *(See Section IV of Appendix "C" of Directive on Privacy Impact Assessment for a list of elements that must be included in the data flow diagram or data flow tables.)*

- 9.3 ☐ AND, if the purposes for which the personal information is used includes any use(s) of the information for a non-administrative purpose, (such as research, statistical, audit and evaluation purposes) the CBSA will adhere to the requirements and principles in the **CBSA Privacy Protocol For Non-Administrative Purposes** (2012), in accordance with section 6.2.15 of the *Policy on Privacy Protection*, to address any impact that such non-administrative uses may have on privacy.

→ Continue to Question 10

NO

- 9.4 ☐ Identify below any other uses of the personal information, in other words, any routine uses that are not directly related to the purpose of the collection, or, which are not consistent with that purpose or for which the information was disclosed to the CBSA pursuant to subsection 8(2) of the *Privacy Act*:

Detail : (This information is mandatory)

- 9.5 ☐ AND, ensure that these other uses are reflected in the relevant **PIB**. (In accordance with subsection 9(1) of the *Privacy Act*, if these other uses are not described in the PIB in CBSA Info Source, the CBSA is required to record each use on the individual's file. Describing them in the PIB is, therefore, a far more efficient practice – see Question 11.)

- 9.6 ☐ AND, include a description of these other uses in the “**Privacy Notice**” or “**Consent Statement**”, as appropriate,

- ☐ AND, ensure the all the other applicable requirements listed under “**YES**” at Question 9 are met.

→ Continue to Question 10

10. Disclosures Directly Related to the Administration of the Program or Activity

Will personal information be disclosed for purposes directly related to the administration of the program or activity?

YES

- 10.1 ☒ Please check all applicable boxes below and, for each disclosure, identify the name of the organization or third party to which personal information will be disclosed. If it is disclosed within the CBSA, please identify the branch and the program or activity.

- 10.1.1 ☒ Within the CBSA for another program or activity

Detail: IOAD and regional intelligence units may collect information from ESDC and subsequently share it with BSOs, CIP, CIU, and IEOD. Also, CIP, CIU, IEOD, IOAD and regional intelligence units may exchange information to support the CBSA's authority to enforce and prosecute offences against the IRPA/IRPR.

- 10.1.2 ☒ Other federal government institutions

Detail: To CIC and ESDC who administer the TFWP/FSWP.

To the Public Prosecution Service of Canada and IRB, when an investigation uncovers information that is referred for prosecution.

10.1.3 ☒ Provincial, territorial or municipal governments institutions

Detail : To Courts/Judges for the application of a search warrant.

10.1.4 ☐ Foreign government institutions and entities thereof

Detail : *(This information is mandatory)*

10.1.5 ☐ International organizations

Detail : *(This information is mandatory)*

10.1.6 ☐ The defence attorney (e.g., contractor or other external service provider)

Detail : The Defence Attorney during pretrial disclosure will disclose for the purposes of the CBSA's authority to prosecute offences against the IRPA/IRPR.

10.1.7 ☒ Other

Detail : To the subjects defence attorney when an investigation uncovers information that is referred for prosecution.

10.2 ☒ AND, ensure that:

- a) any such disclosure is made in compliance with section 8 of the *Privacy Act*, which allows disclosures of personal information with consent of the individual to whom the information relates (subsection 8(1)) or without consent in certain and limited circumstances pursuant to subsection 8(2) of the Act;
- b) only personal information elements that are necessary for the intended purpose are disclosed;
- c) the organization or third party receiving the personal information is authorized to do so;
- d) administrative, physical and technical safeguards appropriate to the sensitivity of the information will be applied to protect the information during and after its transmission (see Question 15);
- e) the organization or third party to which the personal information will be disclosed for the administration of the program or activity are identified in the "Consistent Use" section in the relevant **PIB** in *CBSA Info Source*, including the specific purpose of the disclosure; the "**Privacy Notice**" or "**Consent Statement**" describes any disclosures of information; (For a copy of the CBSA Privacy Notice and Consent Statement template, contact the ATIP Division) and,
- f) the "Data Flow Diagram" or "Data Flow Tables" completed in "*Section 4 – Flow of Personal Information*" of the CBSA PIA include details on the disclosed personal information: (See Section IV of Appendix "C" of *Directive on Privacy Impact Assessment* for a list of elements that must be included in the data flow diagram or data flow tables.)

10.3 ☒ AND, any disclosure of personal information to another federal institution or outside the

Government of Canada is governed by a formal agreement or arrangement (e.g., a Memorandum of Understanding, an accord, a contractual arrangement, etc.) to ensure that appropriate privacy protection clauses are included, and, where applicable, include provisions for inter-jurisdictional or transborder flows of personal information. Such clauses must cover the following topics:

- a) Control over personal information, where appropriate.
- b) Limitations on the collection, retention, use and disclosure of personal information.
- c) Measures (administrative, technical and physical) to protect the integrity and confidentiality of personal information.
- d) Measures governing the disposition of the personal information, where relevant
- e) Measures to ensure or verify that the personal information is only used for the purposes related to the agreement, arrangement or contract.
- f) Obligations are to be extended to other parties such as subcontractors.

→ Continue to Question 11

NO

- 10.4 ☐ There is no disclosure of personal information within or outside the institution for purposes that are directly related to the administration of the program or activity.

→ Continue to Question 11

11. Accounting For New Uses or Disclosures Not Reported in CBSA Info Source

Will controls and procedures be implemented to account for any new use or disclosure of the personal information that is not included in the relevant PIB published in CBSA Info Source?

YES

- 11.1 ☒ Appropriate controls and procedures have been or will be implemented to ensure that:
- a) the head of the institution (The ATIP Director) or the appropriate delegate is notified about any new use or disclosure of personal information that is not reflected in the PIB description published in *CBSA Info Source*;
 - b) the consent of the individual to whom the information relates is obtained in writing, as appropriate, prior to any new use of the information for an administrative purpose that is not reflected in the relevant PIB published in *CBSA Info Source*, unless the new use is considered to be consistent with the purpose for which the personal information was obtained or compiled and the Privacy Commissioner is notified, by the CBSA ATIP Director, forthwith regarding the new consistent use;
 - c) except as permitted under subsection 8(2) of the *Privacy Act*, any disclosure of personal information for a purpose that is not reflected in the relevant PIB published in *CBSA Info Source* will only be made with the consent of the individual to whom the information relates;
 - d) a record is kept for any new use or disclosure of personal information not described in the relevant PIB published in *CBSA Info Source*, and that this record is stored with the personal information to which it relates and retained for a minimum period of two years following such a use or disclosure; *(The record of use or disclosure should include the name and title of the person*

authorizing the use or disclosure; the name of the institution, person, organization or body receiving the information; a description of the use or purpose of disclosure; a copy of the information disclosed, or a description in sufficient detail to allow a determination of exactly what information was used or disclosed.)

- e) if the information is disclosed to a federal investigative body under paragraph 8(2)(e) of the *Privacy Act*, the record of disclosure will be kept in a separate PIB for a period of two years where it will be available to the Privacy Commissioner for review upon request; (e.g., *Standard PIB "Disclosure to Investigative Bodies" PSE 913*)
- f) the Privacy Commissioner is notified, by the CBSA ATIP Director, forthwith, as required under subsection 9(4) of the Act, of any new use or disclosure that is consistent with the purpose for which the information was obtained or compiled, but which is not reflected in the relevant **PIB** published in *CBSA Info Source*;
- g) the relevant **PIB** is amended in time for the next edition of *CBSA Info Source* to include any new use(s) or disclosure(s) that are consistent with the purpose for which the information was obtained or compiled, as well as any routine use(s) or disclosure(s) that do not fall within the categories of purpose of collection or consistent use (e.g., these would include disclosures of the information under subsection 8(2) of the Act that take place on a regular basis. By including these routine uses or disclosures in the PIB, the CBSA would be relieved from the obligation to record each use or disclosure on the individual's file); and
- h) the Privacy Commissioner is notified, by the ATIP Director, prior to or forthwith, as required under subsection 8(5) of the Act, about any disclosures made or to be made in the public interest or in the interest of the individual to whom the information relates.
- i) Other

Detail : *(This information is mandatory)*

→ Continue to Question 12

NO

- 11.2 ☐ Please explain why such controls and procedures will not be implemented

Detail: *Provide adequate justification.*

→ Continue to Question 12

12. Safeguards - Statement Of Sensitivity

Has a Statement of Sensitivity (SoS) or similar analysis been completed to assess the degree of sensitivity of the personal information to be collected and retained for the program or activity? (Input to this section should be coordinated with and reviewed by the CBSA – IT - Security Directorate)

Statutory reference: Sections 7 and 8 of *Privacy Act*.

Policy reference: Appendix C of *Directive on Privacy Impact Assessment* and sections 6.2.17 to 6.2.21 of *Directive on Privacy Practices*, *Policy on Government Security*, *Operational Security Standard: Management of Information Technology Security (MITS)*

YES

- 12.1 ☐ The information contained in the SoS or similar analysis has been taken into account when assessing the level of risks to privacy in "Section 2 - Risk Area Identification and Categorization" of the CBSA PIA.

→ Continue to Question 13

NO

- 12.2 ☒ Please explain why a SoS or similar analysis was not considered necessary to assess the sensitivity of the information.

→ Continue to Question 13

13. Safeguards - Threat and Risk Assessment

Has a Threat and Risk Assessment (TRA) or a similar security assessment been completed for the program or activity? (Input to this section must be coordinated with and reviewed by CBSA – IT - Security Directorate)

Statutory reference: Sections 7 and 8 of *Privacy Act*.

Policy reference: Appendix C of *Directive on Privacy Impact Assessment* and sections 6.2.17 to 6.2.21 of *Directive on Privacy Practices, Policy on Government Security, Operational Security Standard: Management of Information Technology Security (MITS)*

YES

- 13.1 ☐ Reference the title of the TRA or other security assessment in "Section 6 – Supplementary Documents List" and provide a brief synopsis of the assessment in the space below:

Detail : (This information is mandatory)

- 13.2 ☐ AND, obtain assurances from the officials responsible for the program or activity that the measures recommended in the assessment have been implemented to ensure the confidentiality, availability and integrity of the personal information.

- 13.3 ☐ AND, ensure that any residual risks to personal information are known and accepted by the executive or senior official responsible for the program or activity and the Head or delegated authority for the *Privacy Act*. (ATIP Director)

→ Continue to Question 14

NO

- 13.4 ☒ If a TRA or similar security assessment is underway, simply reference that fact in the space below and indicate when it is likely to be completed. If there is no intent to complete one, please explain.

→ Continue to Question 14

14. Safeguards - Administrative, Physical and Technical

Please identify below any administrative, physical and technical safeguards in place, or to be implemented, for this program or activity to ensure the confidentiality, availability and integrity of the personal information. (Safeguards must be commensurate with the sensitivity of the information, the risks identified, and the nature of the media in which the information is stored, handled and transmitted. This section must be completed with input from CBSA – IT - Security Directorate)

Statutory reference: Sections 7 and 8 of Privacy Act

Policy reference: Appendix C of Directive on Privacy Impact Assessment and sections 6.2.17 to 6.2.21 of Directive on Privacy Practices, Policy on Government Security, Operational Security Standard: Management of Information Technology Security (MITS)

Please check all that apply, including safeguards identified by the TRA or similar security assessment.

14.1 Administrative safeguards

- ☒ Internal security and privacy policies and procedures
- ☒ Staff training on privacy and the protection of personal information
- ☒ Screening and security checks of employees
- ☒ Appropriate security levels for employees who will have access to personal information
- ☒ Contingency plans and documented procedures in place to identify and respond to security and privacy breaches, and to communicate security violations to the data subject, law enforcement authorities and relevant program managers
- ☒ Regular monitoring of users' security practices
- ☒ Methods to ensure that only authorized personnel who need to know have access to personal information
- ☐ Other

Detail : (This information is mandatory)

14.2 Physical safeguards

- ☒ Restricted access areas
- ☒ Security guards
- ☒ Identification badges are worn by staff at all times
- ☒ After hours alarms and monitoring systems
- ☒ Locked filing cabinets
- ☒ Combination locks
- ☐ Safes
- ☐ Cipher locks
- ☒ Key cards

- ☒ Video surveillance (closed-circuit television)
- ☒ Secured server locations
- ☒ Backups secured off-site
- ☐ Other

Detail : *(This information is mandatory)*

15. Technology and Privacy - Tracking Technologies

Will the information system(s) used to deliver the program or activity employ cookies or other tracking technologies to collect personal information about users and their transactions? (Input to this section should be coordinated with and reviewed by the CBSA – IT - Security Directorate)

Statutory reference: Sections 4 to 10 of the Privacy Act and section 4 of Privacy Regulations

Policy reference: Subsections 6.1.1, 6.1.3, 6.1.9, 6.2.9 to 6.2.13, 6.2.17 and 6.2.23 of Directive on Privacy Practices

YES

- 15.1 ☐ The specific tracking technologies to be used is adequately described under Part 6: Technology and Privacy of "Section 2 – Risk Area Identification and Categorization" of the CBSA PIA; (For example, the use of an audit trail that records information, such as user logon ID, date and time of logon, logout, user location, terminal identity, name and ID of client records accessed, including edits or changes

made during each user session, etc. The information is used to verify that only authorized users access personal information and to ensure that access can be linked to specific individuals to support the investigation of suspected or alleged misuse. The information is retained for a period of two years.)

- 15.2 ☐ AND, the collection of any personal information using such technologies is reflected in the relevant **PIB** and in "Section 3 – Analysis of Personal Information Elements" of the CBSA PIA;
- 15.3 ☐ AND, the use of such technologies to collect information about users and their transactions is adequately reflected in the "Privacy Notice";
- 15.4 ☐ AND, those responsible for implementing and using tracking technologies to collect personal information or who may have access to personal information collected through these methods are made aware of privacy and security policy requirements;
- 15.5 ☐ AND, where personal information collected through such tracking technologies is used to make a decision that directly affects the individual to whom the information relates, it will be retained for a minimum of two years after the last administrative action as required under the *Privacy Regulations*.

→ Continue to Question 16

NO

- 15.6 ☒ Tracking technologies are not used to collect personal information about users.

→ Continue to Question 16

16. Technology and Privacy - Surveillance or Monitoring

Will the new or modified program or activity result in new or increased surveillance or monitoring of a targeted population? (Input to this section should be coordinated with and reviewed by the CBSA – IT - Security Directorate)

Statutory reference: Sections 4 to 10 of *Privacy Act*, section 4 of *Privacy Regulations* and section 8 of the *Charter of Rights and Freedoms*

Policy reference: Subsections 6.1.1, 6.1.9, 6.2.9 to 6.2.13 and 6.2.17 of *Directive on Privacy Practices*

YES

- 16.1 ☐ Consult with your legal advisors to determine whether or not such surveillance or monitoring activities raise any issues relating to the *Charter of Rights and Freedoms*, the *Privacy Act* or other applicable acts.
- 16.2 ☐ And, ensure the surveillance or monitoring method(s) to be used, the characteristic(s) of the targeted population and the scope of the surveillance or monitoring are adequately described under Part 6: Technology and Privacy of "Section 2 – Risk Area Identification and Categorization" of the CBSA PIA.
- 16.3 ☐ AND, any personal information collected or created as a result of such surveillance or monitoring is described in the relevant **PIB** and in Section 3 – Analysis of Personal Information Elements" of the CBSA PIA.
- 16.4 ☐ AND, the collection or use of personal information through surveillance or monitoring is adequately reflected in the "Privacy Notice", unless such notification might result in the collection of inaccurate information or defeat the purpose or prejudice the use for which the personal information is collected.

☐ If notice about surveillance or monitoring will not be provided

Detail explain why: *(This information is mandatory)*

- 16.5 ☐ AND, those responsible for implementing and using such surveillance or monitoring method(s) or who may have access to personal information collected or created through these methods are made aware of privacy and security policy requirements.

→ Continue to Question 17

NO

- 16.6 ☒ The new or modified program or activity will not result in surveillance or monitoring.

→ Continue to Question 17

17. Considerations Related to Compliance, Regulatory Investigation, Enforcement

Does the program or activity involve compliance/regulatory investigation or law enforcement, surveillance or intelligence gathering that targets specific individuals against whom penalties, criminal charges or sanctions may be applicable?

YES

- 17.1 ☒ Consult with your legal advisors to determine whether or not the compliance/regulatory investigation or law enforcement activities raise any issues relating to the *Charter of Rights and Freedoms*, the *Privacy Act* or other applicable acts.

- 17.2 ☒ AND, identify the legislative authority and the specific regulatory or law enforcement purpose involved:

Detail: Subsection 4(2) of the IRPA states the Minister of Public Safety and Emergency Preparedness is responsible for administering the Act as it relates to the enforcement of the Act, including arrest, detention and removal.

- 17.3 ☒ AND, if the legislative authority differs from the legal authority for the program or activity, ensure it is adequately reflected in the response to Question 1 of "Section 5 – Privacy Compliance Analysis" and in "Section 1 – Overview and PIA Initiation" of the CBSA PIA.

- 17.4 ☒ AND, any personal information collected or created as a result of such regulatory or criminal enforcement, surveillance or intelligence gathering program or activity is described in the relevant **PIB** and in "Section 3 – Analysis of Personal Information Elements" of the CBSA PIA.

- 17.5 ☒ AND, the collection or use of personal information through these compliance / regulatory investigation or enforcement activities is adequately reflected in the "**Privacy Notice**", unless such notification might result in the collection of inaccurate information or defeat the purpose, or prejudice the use, for which the personal information is collected.

- ☐ If notice about the compliance/regulatory investigation or law enforcement activities will not be provided.

Details explain why: *(This information is mandatory)*

NO

- 17.6 ☐ The program or activity does not involve the conduct of regulatory or criminal enforcement, surveillance or intelligence gathering.

SECTION 6 - Summary of Analysis and Recommendations

The ATIP Division will document the recommendations resulting from the risk identification and categorization, as well as in a manner that is commensurate with the risk identified. The risks and recommendations will be incorporated into the action plan as described in Annex B: Office of the Privacy Commissioner Expectations (2011)

Document the conclusion drawn or recommendations resulting from the risk identification and categorization in a manner that is commensurate with the risk identified.

ACCOUNTABILITY

Within the CBSA

The CBSA has a robust administrative structure to ensure compliance with the *Privacy Act* and related policies and directives. In FY 2012-2013, a Privacy Oversight Committee (POC) was established which consists of senior officers and executives within the CBSA that meet regularly to discuss privacy issues, as well as monitor the development of privacy policy instruments and PIAs. The POC also helps identify a need to assess upcoming initiatives for potential PIAs.

Bi-monthly reports on the status of PIAs are provided routinely to the POC and the OPC to ensure adequate planning for the completion of PIAs.

The ATIP Division is responsible for recommending the development of a PIA and/or other measures to ensure that existing or new programs / activities are privacy compliant. When contacted, the ATIP Division will provide program areas with the Privacy Impact Questionnaire (PIQ). The PIQ is a template that requests high-level information similar to sections 1 and 2 of the Core PIA template, and is used to develop and record any recommendations given by the ATIP Division concerning the program or activity. The PIQ enables the ATIP Division to make informed recommendations as to whether or not a PIA or other privacy compliant measures are required.

The ATIP Division is also a required stakeholder in the development of Written Collaborative Arrangements (WCAs) such as MOUs and ISAs. Aside from reviewing WCAs for compliance with the *Privacy Act* and TBS policies, directives, and guidelines, the ATIP Division also makes recommendations with respect to the conduct of a PIA before the implementation of WCAs.

In FY 2012-2013, the CBSA also developed two privacy policy instruments:

- The Privacy Breach Protocol; and
- The Directive on Non-Administrative Uses of Personal Information (Privacy Protocol)

The Privacy Breach Protocol ensures that all security violations which include personal information are reported to the ATIP Division in addition to the Security and Professional Standards Division, and outlines the roles and responsibilities of the Agency with respect to privacy breaches, which may include notification of the individuals, notification of the OPC, and the identification of mitigating measures.

The Directive on Non-Administrative Uses of Personal Information sets out the process, roles and responsibilities for the creation of a Privacy Protocol for those programs and initiatives the use personal information for non-administrative purposes, such as statistical reporting.

In FY 2013-2014 the CBSA introduced an online awareness course on Information Management (IM) and ATIP. The course was jointly developed in FY 2012-2013 and seeks to educate employees on their IM and ATIP responsibilities. This course will be supplemented by current training activities, which include an in-depth session on the administration of the ATIP program at the CBSA, the development of PIAs, and Info Source training.

Specific to TFWP and the ISA with ESDC

The ISA between the CBSA and ESDC maintains strict clauses related to the types of information that is permitted to be exchanged, the method of exchange, security of information, accuracy, secondary disclosures, authorities for disclosure, and audit capabilities.

Also, the ISA stipulates that each organization has designated a senior manager for issues related to the implementation and administration of the agreement.

Risks and Mitigations Strategies

No risks have been identified related to this principle.

IDENTIFYING PURPOSES

Within the CBSA

The CBSA maintains its *Info Source* chapter on its website at <http://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/pia-efvp/atip-aiprp/infosource-eng.html>. It conducts ongoing reviews of the chapter to ensure that it accurately and completely describes the personal information activities of the Agency.

Specific to TFWP

PIB CBSA PPU 050 (TFWP), CBSA PPU 035, and CBSA PPU 1402 accurately reflect the types of information collected, the purpose, legislative authority, and the consistent uses of the information, including the disclosure of information to CIC and ESDC for the purposes of administering the TFWP/FSWP.

Risks and Mitigations Strategies

No risks have been identified related to this principle.

CONSENT

Within the CBSA

The ATIP Division works with program areas as necessary to develop adequate consent statements and forms as part of the PIA process or as requested by CBSA program areas.

Specific to TFWP

Consent is obtained from the FN at the time he/she reports to a POE with the appropriate documentation. The individual reports for examination and when applicable submits an E-311 form which contains proper notice instructions. The individual has also been provided with adequate privacy notice provisions related to the Work Permit and has provided implied consent within the LMIA Application process.

Also, by seeking inclusion in the TFWP/FSWP, the FN understands that his/her personal information may be used to administer and enforce the IRPA and IRPR, of which the CBSA has certain responsibilities.

Risks and Mitigations Strategies

No risks have been identified related to this principle.

LIMITING COLLECTION

Within the CBSA

Throughout the PIA process, the ATIP Division works with program areas to ensure that CBSA programs limit the collection of personal information to only that which is necessary to administer the program or activity.

Specific to TFWP

The ISA between the CBSA and ESDC enumerates the data elements that can be exchanged. However, as this ISA allows for information to be used for additional purposes than what has historically been permitted, it is important that CBSA staff understand the types of information which they can request, collect, and use. Furthermore, because the CBSA is negotiating further expansion of data exchange with ESDC, it is important that staff within CIP, CIU, IEOD, IOAD, and regional intelligence units are aware of the current limitations on what data can be requested and disclosed. In other words, that the current structure of the ISA does not permit CBSA staff to request or disclose information that is being negotiated for further expansion of the ISA.

Risks and Mitigations Strategies

Risk #1: There is a risk that personal information could be disclosed to/by the CBSA and used for a purpose that is beyond the scope of the ISA. Furthermore, there is a risk that CBSA staff may be unaware of the limitations of the ISA and that an offence provision within DESDA may apply to them and the CBSA if they disclose information received from ESDC in contravention to the ISA/DESDA.

Mitigation: All relevant staff will be made aware of the parameters of the ISA and that disclosures to/by the CBSA must be limited to those authorized under the current ISA. Operational guidance will be developed and provided to staff that outlines the limitations of the ISA, as well as the applicable offence provisions within DESDA. In addition, measures to appropriately identify ESDC information held within CBSA systems will be introduced.

LIMITING USE, DISCLOSURE AND RETENTION

Within the CBSA

Throughout the PIA process, the ATIP Division works with program areas to ensure that CBSA programs limit the use, disclosure, and retention of personal information to only that which is necessary to administer the program or activity.

In FY 2012-2013, the CBSA developed guidelines on the disclosure of customs information pursuant to s.107 of the *Customs Act*. These guidelines set out the specific provisions, their limitations, relevant considerations and the appropriate positions within the CBSA (employee, supervisor, senior manager) that can authorize specific disclosures or uses. Personal information that is also customs information is disclosed in accordance with s.107 of the *Customs Act* rather than ss. 8(2) of the *Privacy Act*.

A similar set of guidelines for s. 8(2) of the *Privacy Act* was implemented in FY 2013-2014.

Specific to TFWP

The ISA between the CBSA and ESDC enumerates the data elements that can be exchanged, as well as the use and disclosure restrictions. To abide by the ISA, it is important for CBSA staff to be able to identify information which has been provided by ESDC so that such information can be subjected to the strict secondary disclosure requirements of the ISA. However, when data is provided through ESDC's Online Fraud Reporting Tool, requested and provided IEOD, IOAD, and regional intelligence units there are limited mechanisms within the CBSA to identify/mark the electronic information or the hard copy information as having been disclosed by ESDC. Therefore, it will be difficult for the CBSA to apply the secondary disclosure restrictions that are reflected in the ISA.

Risks and Mitigations Strategies

Mitigation: The CBSA will implement procedures to clearly identify ESDC records that are shared pursuant to the ISA. This will apply to both paper records and data that are stored in CBSA systems.

Furthermore, BSOs will be made aware that restrictions to the sharing of ESDC information also apply to information obtained via the FWS-FOSS/FWS-GCMS one way interface.

ACCURACY

Within the CBSA

Throughout the PIA process, the ATIP Division works with program areas to ensure that CBSA programs create a process for ensuring the accuracy of information as required, and that program areas are capable of handling requests for correction of personal information.

The correction process is coordinated centrally from the ATIP Division. Requests for correction are forwarded to the appropriate program area for action. A response letter is sent to the client indicating whether the correction was accepted or refused, whether the correction is made directly or notated to the file, and whether or not that information has been disclosed and that those recipients would be informed appropriately. The ATIP Division is looking at developing a more standardized approach and directive in FY 2013-2014 for the processing of correction requests.

Specific to the TFWP

TFWs who present themselves at the POE with a WP, positive LMIA report, or other documentation have their personal information matched with GCMS, which maintains an interface with FWS. Therefore, as with other identity matching procedures at the CBSA, BSOs are diligent in ensuring that the FN presenting him/herself at the POE is the same individual who has applied to CIC and/or ESDC for inclusion in the TFWP.

Regarding the activities of CIP, CIU, IEOD, IOAD, and regional intelligence units, as part of their investigative and intelligence activities, procedures are in place to ensure accuracy of information before an administrative action is taken against the individual.

Risks and Mitigations Strategies

No risks have been identified related to this principle.

SAFEGUARDS

Within the CBSA

Typically the ATIP Division strongly recommends the completion of a TRA and SoS as part of the PIA process, and directs programs to contact Corporate Security for guidance with respect to those instruments. A summary of the risks identified in a TRA are appended to the PIA to ensure that all risks are identified and mitigated by the program area.

CBSA employees are required to take the online CBSA Security Awareness course when they begin employment, and to refresh their training every two years. CBSA managers are required to take both the CBSA Security Awareness course and a CBSA Security Awareness course for managers.

The Privacy Breach Protocol complements existing CBSA security policies, and ensures that all security violations which include personal information are reported to the ATIP Division in addition to the Security and Professional Standards Division, and outlines the roles and responsibilities of the Agency

with respect to privacy breaches, which may include notification of the individuals, notification of the Office of the Privacy Commissioner, and the identification of mitigating measures.

Specific to TFWP

All relevant information systems at the CBSA have been through the Security Assessment and Authorization (SA&A) process (formerly the Certification and Accreditation) for the processing and storing of Protected B information.

Regarding the ISA, ESDC is responsible for developing and maintaining
 As ESDC is responsible for maintaining
 CBSA will ensure that no information is uploaded to the site
 until such time that appropriate security measures are in place.

Separate from some data is This practice may change once
 the is in place; however, the : may involve information classified as Protected
 B or higher that must be sent via approved methods. Also, emails exchanged between CBSA
 investigators and ESDC's TFWP regarding requests for paper copies of LMIA data (to support search
 warrants and prosecution) that is related to an ongoing investigation at CBSA should be considered
 Protected B information; these email transmissions may require

Risks and Mitigations Strategies

Risk #5: When information is needed by the CBSA to support legal proceedings (i.e. prosecution), a request is sent to ESDC's TFWP However, there may be instances where with investigative details designated as information are sent to ESDC

OPENNESS

Within the CBSA

The CBSA manages its Info Source chapter directly on the CBSA website at <http://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/pia-efvp/atip-aiprp/infosource-eng.html>. The ATIP Division ensures that the descriptions of program privacy practices are kept complete and up-to-date.

The Directive on Privacy Impact Assessments requires departments to ensure that PIA summaries in both official languages are made available to the public. At a minimum the summary must address section 1 and 2 of the Core PIA Template. CBSA PIA summaries are posted at <http://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/pia-efvp/atip-aiprp/pias-sefp-eng.html>.

Upon completion of a PIA, PIA summaries are posted on the CBSA website, which also contains information on accessing personal information at the CBSA.

Specific to TFWP

PIB CBSA PPU 050 (TFWP), CBSA PPU 035, and CBSA PPU 1402 accurately reflect the types of information collected, the purpose, legislative authority, and the consistent uses of the information, including the disclosure of information to CIC and ESDC for the purposes of administering the TFWP/FSWP.

Also, a PIA Summary will be authored and submitted to CBSA ATIP for approval and posting on the CBSA website.

Risks and Mitigations Strategies

No risks have been identified related to this principle.

INDIVIDUAL ACCESS

Within the CBSA

The CBSA maintains a robust and responsive ATIP program. The ATIP Division implemented a more rigorous records retrieval process in November 2011. The process improved the accountability of records retrieved by actively engaging CBSA directors. In combination with the ATIP Division's training regime, CBSA employee and management ATIP awareness has increased considerably.

Specific to the TFWP

When required, BSOs and all relevant staff involved in TFWP/FSWP respond accordingly to ATIP requests.

Risks and Mitigations Strategies

No risks have been identified related to this principle.

CHALLENGING COMPLIANCE

Within the CBSA

The ATIP Division is primarily responsible for coordinating responses to privacy complaints that were submitted to the OPC. Incoming complaints are assigned to an ATIP officer, who in turn tasks the appropriate program area to provide records relevant to the complaint, draft a response to the complaint, and if necessary, institute measures to resolve the complaint (if a response is not sufficient).

The ECM program is responsible for coordinating responses to service-related complaints received via the online feedback form.

Specific to TFWP

When required, BSOs and all relevant staff involved in TFWP/FSWP respond accordingly to ATIP requests.

Risks and Mitigations Strategies

No risks have been identified related to this principle.

Summary of Identified Risks:

Principle	Risk #	PIA Section	Details
1 - Accountability	N/A		
2 - Identifying Purposes	N/A		
3 - Consent	N/A		
4 - Limiting Collection	1	Introduction/Annex J Sections 4.2 and 4.3	<p>There is a risk that personal information could be disclosed to/by the CBSA and used for a purpose that is beyond the scope of the ISA. Furthermore, there is a risk that CBSA staff may be unaware of the limitations of the ISA and that an offence provision within DESDA may apply to them and the CBSA if they disclose information received from ESDC in contravention to the ISA/DESDA.</p> <p><u>Mitigation:</u> All relevant staff will be made aware of the parameters of the ISA and that disclosures to/by the CBSA must be limited to those authorized under the current ISA. Operational guidance will be developed and provided to staff that outlines the limitations of the ISA, as well as the applicable offence provisions within DESDA. In addition, measures to appropriately identify ESDC information held within CBSA systems will be introduced.</p>
	2	Section 4.3	<p>There is a risk that information obtained from ESDC pursuant to the ISA may be disclosed to a third party in contravention of the disclosure clauses of the ISA. Currently, information received from ESDC may not be appropriately identified/marked as originating from ESDC, and subject to the unique disclosure restrictions of the DESDA.</p> <p><u>Mitigation:</u> The CBSA will implement procedures to clearly identify ESDC records that are shared pursuant to the ISA. This will apply to both paper records and data that are stored in CBSA systems. Furthermore, BSOs will be made aware that restrictions to the sharing of ESDC information also apply to information obtained via the FWS-FOSS/FWS-GCMS one way interface.</p>
7 - Safeguards	3	Introduction Section 5 (Question 13)	which will be used by ESDC and the CBSA

Principle	Risk #	PIA Section	Details
			to exchange Protected B information.
	4	Section 4.3	<p>The current disclosure of information by ESDC to the CBSA via the Online Fraud Reporting Tool is not transmitted to the CBSA</p> <p>When ESDC staff complete the CBSA Lead Referral Form, it may</p>
	5	Section 4.3	<p>When information is needed by the CBSA to support legal proceedings (i.e. prosecution), a request is sent to ESDC's TFWP via . However, there may be instances where with investigative details designated as Protected B information are sent to ESDC v</p> <p><u>Mitigation:</u> The CBSA and ESDC will make every reasonable effort to ensure that the transmission of information via utilizes , when it is necessary.</p>
8 - Openness	N/A		
10 - Challenging Compliance	N/A		

SECTION 7 - SUPPLEMENTARY DOCUMENTS LIST

List all supplementary documents that support the conclusions of this CBSA Privacy Impact Assessment. For each document, cite the specific sections of the documents (subject, chapter, page, paragraph, etc.) that correspond with the CBSA PIA and link them to the PIA sections.

Document	Document Reference	PIA Reference
Information Sharing Agreement	Entire Document	Scope of the PIA is related to this PIA
2011 PIA on MOU (Data Sharing for TFWP Between ESDC and the CBSA)	Entire Document	Introduction, Section D

SECTION 8 - FORMAL APPROVAL

The following signature represents a commitment to comply with sections 4 to 8 of the *Privacy Act* and the related privacy policy requirements outlined in the CBSA PIA as they relate to the administration of the identified program or activity.



Peter Hill, A/Vice President, Programs Branch

OCT 23 2015

OCT 23 2015

Date

Note: Responsibility for sections 4 to 8 of the *Privacy Act* rests with all employees of government institutions that handle personal information. Officials who manage such programs and activities are responsible for ensuring that such requirements are implemented as part of the administration of the program or activity.

The following signature represents a commitment by the Head of the institution or his/her delegate(s) who is responsible for establishing personal information banks in accordance with section 10 of the *Privacy Act*.



Dan Proulx, ATIP Director

OCT 20 2015

Date

Note: Under the *Privacy Act*, the Head or his/her delegate(s) is responsible for complying with legal and relevant privacy policy requirements related to the approval and registration of personal information banks

Annex A: Privacy Compliance Checklist and Other Considerations

Note: The table below must be used to keep an account of actions completed and to track outstanding actions required to achieve privacy compliance:

Privacy Compliance Analysis question #	Action required to support legal and policy compliance (cross reference to relevant question of <i>Section 5 – Privacy Compliance Analysis</i>)	Done	To be done
1	Legal authority for the program or activity has been established and is reflected in the relevant PIB.	<input checked="" type="checkbox"/>	<input type="checkbox"/>
2	a) The categories and elements of personal information to be collected for the new program or activity have been carefully assessed based, for example, on the CBSA's experience gained with the administration of a similar program or activity. The personal data collected will be limited to only that which is required.) b) Categories and elements of personal information have been described in the relevant PIB for the program or activity. c) Controls and procedures will be implemented to ensure the CBSA does not collect more personal information than necessary for the program or activity and that a continuing need exists for the personal information and its collection.	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>
4 and 5	a) All of the requisite "Privacy Notices" and "Consent Statements" that meet the requirements of sections 6.2.9 to 6.2.12 of the <i>Directive on Privacy Practices</i> have been drafted. (Texts of the notices and consent statements must be included as an annex.) For a copy of the CBSA Privacy Notice and Consent Statement template, contact the ATIP Division. b) Controls and procedures have been implemented to keep records of individual consents, and to ensure that persons acting on behalf of individuals who do not have the capacity to provide consent have the authority to do so under section 10 of the <i>Privacy Regulations</i> .	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/>
7	a) A Records Disposal Authority (RDA) has been approved by Library and Archives Canada to authorize the disposal of the records containing personal information for the program. b) Controls and procedures have been implemented within the program or activity and the CBSA ATIP Division to ensure that information that has been used for an administrative purpose will be kept for the minimum retention period established by the Privacy Regulations. c) Reference to the RDA, the retention period and the disposition standards for the program have been cited in the relevant PIB.	<input checked="" type="checkbox"/> <input checked="" type="checkbox"/> <input checked="" type="checkbox"/>	<input type="checkbox"/> <input type="checkbox"/> <input type="checkbox"/>

Privacy Compliance Analysis question #	Action required to support legal and policy compliance (cross reference to relevant question of <i>Section 5 – Privacy Compliance Analysis</i>)	Done	To be done
8	Controls and procedures are in the process of being implemented to ensure that the personal information associated with the program is as accurate, complete and up-to-date as necessary.	<input checked="" type="checkbox"/>	<input type="checkbox"/>

**Other Privacy Considerations related to specific principles that are not explored in the previous 17 sections:
(these considerations should be explored in the Executive Summary)**

Openness	Describe how the results of any privacy impact assessment or audit will be made available to the public. The Executive Summary will be published on the external CBSA ATIP Division website at http://www.cbsa-asfc.gc.ca/agency-agence/reports-rapports/pia-efvp/atip-aiprp/pias-sefp-eng.html	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Are policies and practices relating to the proposal's management and handling of personal information available to the public?	<input type="checkbox"/>	<input type="checkbox"/>
	Is there a communications plan to explain to the public how personal information will be managed and protected?	<input type="checkbox"/>	<input type="checkbox"/>
	Is there a clearly defined and easy process for individuals to access such information and/or communicate with appropriate individuals with respect to policies and practices relating to management and protection of personal information?	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Where appropriate, will public consultation take place on the privacy implications of the proposal? N/A	<input type="checkbox"/>	<input type="checkbox"/>
Individual's Access to Personal Information	Is the system designed to ensure that an individual can have access to his/her personal information, including all other programs or applications that have received copies of the information? s. 12(1)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Are there documented procedures developed or planned on how to make privacy requests or requests for the correction of personal information? s. 12 (2)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Are individuals provided with access to their personal information in the official language of their choice? s. 17(2)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	If appropriate, are individuals provided with access to their personal information in an alternative format? s. 17(3)	<input checked="" type="checkbox"/>	<input type="checkbox"/>
Challenging	Are the complaint procedures for the proposed program or service	<input checked="" type="checkbox"/>	<input type="checkbox"/>

Privacy Compliance Analysis question #	Action required to support legal and policy compliance (cross reference to relevant question of <i>Section 5 – Privacy Compliance Analysis</i>)	Done	To be done
Compliance	consistent with legislated requirements? s. 29-35		
	To improve information management practices and standards, has a procedure been established to log and periodically review the nature, frequency and resolution of complaints?	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Are there oversight and review mechanisms implemented or available to ensure accountability?	<input checked="" type="checkbox"/>	<input type="checkbox"/>
	Have oversight agencies, including the Office of the Privacy Commissioner, issued reports or opinions on issues that would be relevant to the proposal? N/A	<input type="checkbox"/>	<input type="checkbox"/>

Annex B: Office of the Privacy Commissioner Expectations

In their March 2011 document, *Expectations: A Guide for Submitting Privacy Impact Assessments to the Office of the Privacy Commissioner of Canada*, the Office of the Privacy Commissioner (OPC) has expressed the importance of analysing the risks of the project, program or initiative against the ten universal privacy and fair information practice principles of the Canadian Standards Association Model Code for the Protection of Personal Information.

The most relevant demonstration of the privacy risk and compliance analysis is the action plan. The OPC has said the following in their **Expectations** guide with respect to the action plan:

Once privacy risks and their proposed mitigating measures have been identified, we expect to see an Action Plan drawn up by the institution, indicating a specific time frame for remedying or mitigating the risks that have been identified, and if possible, naming a specific person or staff position accountable for taking action.

The action plan must list all privacy risks and compliance issues identified in the PIA and supplementary documentation. All risks and issues must be organized by the 10 universal privacy principles.

All recommendations and proposed mitigation strategies must also be described in the action plan. Identify the responsible program area and the timeline for completion or implementation of the strategy. The ATIP Division will provide programs with an action plan template to be addressed near the end of the PIA process.

The expectations of the OPC for each privacy principles are included below for your reference.

Accountability

Under this principle the OPC would expect to see documentation of an administrative structure for privacy, including input from legal services, access to information and privacy and information technology branches within an institution, with defined processes for determining when new projects require PIAs, for carrying them out, implementing mitigating measures and auditing for assurance of compliance. We expect PIA reports to be signed off at the appropriate level, and that training in privacy issues and procedures has been documented and is refreshed with employees regularly; and that privacy protective language is included in all contracts with third parties handling personal information in accordance with TBS guidance documents and internationally accepted best practices; and that regularly scheduled privacy compliance audits will be undertaken and the findings acted upon.

Identifying Purposes

The *Privacy Act* restricts federal government institutions to the collection of personal information that relates directly to an operating program or activity of the institution, so we would expect to see a clear description of the program and why each piece of information is needed; a description of the legislative authority for the collection; a clear listing of all the data elements collected; copies of any relevant documents such as application forms identifying the purpose for the collection or on-line notices of use; a copy of an up to date Personal Information Bank (PIB) description; a statement of any proposed new consistent use of information previously collected and a clear rationale as to how the use is reasonable

and directly connected to the original collection -- this may include an analysis of how an individual to whom it relates would reasonably expect it to be used for that purpose; a statement outlining any intended secondary uses of the information; whether the information is collected directly from the individual and if not, why; and a description of how personal information used for planning, forecasting or statistical purposes would be anonymized or de-linked from individual identifying information.

Consent

This is closely tied to the Identifying Purpose principle. Under this principle, OPC would expect to see a copy of notification language on forms or websites; a clear description of the purpose for collection; a rationale for not seeking consent, as is provided for in the Privacy Act; for web sites, a copy of the Privacy Notice Statement under which personal information is submitted to the institution.

Limiting Collection

Under this principle, OPC would expect to see a clear justification of the need for each data element collected, in keeping with the requirement of the Privacy Act that no personal information is to be collected by a government institution unless it relates directly to an operating program or activity of the institution; an indication that a data minimization exercise has been undertaken to ensure that each data element is necessary and that this exercise will be refreshed regularly; and that information collected from another department for a secondary use will be purged of all but the essential data elements before use.

Limiting Use, Disclosure and Retention

Under this principle, OPC would expect to see a description of the specific uses and proposed disclosures of the information; a clear statement limiting the use of the information to the purposes identified; a clear retention policy and disposition schedule that is also noted in the PIB; a process for destruction of the information that is in keeping with the Privacy Act and Regulations; copies of MOUs or agreements with third parties to whom information is disclosed governing its use, retention and disclosure, and clauses with contractors or sub-processors of information indicating the originating institution has the right to audit for compliance with privacy provisions.

Accuracy

Under this principle, OPC would expect to see a description of the process used by entities to ensure accuracy, particularly when administrative decisions are made; a description of how changes to records are logged and monitored; a statement of whether automated decision-making based on risk profiles is being undertaken and how automated decisions are vetted for accuracy; an explanation of the processes open to individuals seeking to correct information; a description of the process by which second or third parties to whom information has been disclosed will be notified of changes and corrections to the record; and a description of how audit trails of records transactions are monitored and evaluated.

Safeguards

OPC would expect to see under this principle a description of the physical and electronic safeguards that are in place to protect information; a Threat & Risk Assessment (TRA) with emphasis on privacy risks and concerns and a discussion of how these concerns have been remedied or addressed; a notation that encryption is used for personal information both in transit and at rest; a description of how system logs of information transactions are monitored for inappropriate use, including viewing of the information; strong electronic access control, including controls on remote access, and the use of mobile devices;

policies for the use of portable storage devices such as flash drives; a description of role-based access controls; and a description of the steps taken to ensure complete destruction of the information at the end of its life cycle.

Openness

Under this principle, OPC would expect to see a summary of the PIA written in plain, understandable language, posted on the institutional website in a manner accessible to the general public and containing a link to the relevant PIB description in CBSA Info Source; for particularly sensitive or privacy invasive programs we would expect to see the public communications plan described in the PIA, including a variety of methods such as posters, brochures and media announcements as well as detailed discussion of the PIA in the institution's Annual Report under the Privacy Act; a description of consultations with key stakeholders and the privacy risks or concerns raised should be readily available on the website; the name and contact information of an individual accountable for the handling of personal information should be easily obtained through the website or by calling the institution's main public number.

Individual Access

Under this principle, OPC would expect the PIA to include a description of any informal process the CBSA may have in place for access to and correction of personal information; an up to date and comprehensive description of information contained in the PIB corresponding to the initiative; a description of the process by which information in the hands of third parties is corrected following requests; a description of how the general public is made aware of these processes, for example, by a link and/or a toll-free number shown on the home page of the institutional website.

Challenging Compliance

OPC would expect to see the PIA address this principle by indicating clearly who is responsible for receiving and resolving privacy complaints; describing complaints that may have been received in any similar activity or pilot project and how they were handled; including privacy issues in project evaluations or feasibility reports; describing how and when compliance audits for privacy will be undertaken; including information on how to file a complaint with OPC under the Privacy Act; and reporting in some detail on specific and/or systemic privacy issues in its Annual Reports.

Annex C: Categories of Personal Information

The **Description** section in a personal information bank (PIB) describes the personal information in the records to which the bank relates. Treasury Board Secretariat has established the following categories of personal information, which give examples of specific elements of personal information that fall under each category. The purpose of the categories is to reduce the number of personal information elements that need to be listed in the Description section. These categories are representative of the personal information collected by most institutions, and they now appear in many of the CBSA registered PIBs. The ATIP Division modified the original list to reflect CBSA business lines.

- Biographical information (e.g. work history, curriculum vitae, family information, Passenger Information, etc.)
- Biometric information (e.g. blood type, eye or facial scan, DNA, finger / hand prints, etc.)
- Contact information (e.g. work and / or home information, including postal and e-mail addresses, telephone, fax, cell phone numbers, etc.)
- Citizenship status or Nationality (e.g. citizen, landed immigrant, etc.)
- Crew detailed information
- Criminal checks / history (e.g. information related to criminal record checks, investigations, charges, conviction dates and locations, pardons, etc.)
- Date of birth
- Date of death
- Destination City
- Employee identification number (e.g. Personal Record Identifier)
- Employee personnel information (e.g. records of attendance and leave, notices of disciplinary action, alternative work arrangements, decisions concerning compensation and fitness for work, official languages qualifications, salary, deductions, level of security clearance, performance reviews and appraisals, rating board assessments, including evaluation notes from staffing boards, training and development course applications and evaluations, etc.)
- E-Ticket Information
- Financial information (e.g. income, investments, mortgages, loans, orders of garnishment, financial institution information for direct deposit and other banking purposes, including name and branch number of institution, account number(s) and name(s) on accounts, etc.)
- FOSS Case Number
- Gender
- Itinerary Cities
- Language (e.g. mother tongue, official and other languages, etc.)
- Medical information (e.g. psychological assessments, blood type, etc.)
- Name (e.g. last name (surname/family name), given names (first, second or more), maiden name, nicknames, aliases, etc.)
- Opinion or views of, or about, individuals
- Passenger Name
- Passport Number or Travel Document Number

- Place of ticket purchase
- Photos
- Physical attributes (e.g. height, weight, color of hair and eyes, physical markings (scars, tattoos, body piercing), etc.)
- Place of birth
- Place of death
- Port of Embarkation and Port of Debarkation
- Signature
- Special Travelling Considerations such as Employee Pass, Buddy Pass and Parental Passes
- Visa Number

Annex D: Labour Market Impact Analysis Application



Employment and Social Development Canada
Emploi et Développement social Canada

Please Print
PROTECTED WHEN COMPLETED - B

LABOUR MARKET IMPACT ASSESSMENT APPLICATION HIGH-WAGE AND LOW-WAGE POSITIONS

Employers should visit the Temporary Foreign Worker Program TFWP website at www.esdc.gc.ca/eng/jobs/foreign_workers/index.shtml, to verify that the Program is accepting applications for the specific occupation or sector for which they wish to hire the temporary foreign worker (TFW) and to determine if they are eligible to participate in the Program.

Personal Information Collection Statement

The information you provide on this form is collected by Employment and Social Development Canada (ESDC) under the authority of the *Immigration and Refugee Protection Act* (IRPA) and *Immigration and Refugee Protection Regulations* (IRPR), for the purpose of providing a Labour Market Impact Assessment (LMIA) in accordance with these statutes. Completion is voluntary; however, failure to complete this form will result in your LMIA application not being processed.

The information you provide may also be shared with Citizenship and Immigration Canada (CIC) for the administration and enforcement of the IRPA and IRPR as permitted by the *Department of Employment and Social Development Act* (DESD Act), and may be accessed by the Canada Border Services Agency (CBSA) for the purpose of issuing work permits at Ports of Entry. ESDC may also provide information to CBSA in order for that agency to investigate and enforce the IRPA and IRPR in relation to an LMIA.

The information may also be shared with provincial/territorial governments for the purpose of administration and enforcement of provincial/territorial legislation, including employment standards and occupational health and safety legislation, as permitted by the DESD Act. The information may also be used by ESDC for inspections, policy analysis, research and evaluation in relation to the entry and hiring of TFWs to Canada or the IRPA.

The information you provide is administered under Part 4 of the DESD Act and the *Privacy Act*. You have the right to access and request correction of your personal information, which is described in Personal Information Bank PPU 440 and PPU 171 of Info Source. Instructions for making formal requests are outlined in the Info Source publication available online at infosource.gc.ca.

A person, who contravenes a provision set out under sections 126 or 127 of the *Immigration and Refugee Protection Act* (misrepresentation), could be liable to a fine or to imprisonment, or to both. Also, providing inaccurate information, in the context of this application, may lead to an administrative penalty such as being ineligible to access the Program for a period of two years.

BUSINESS INFORMATION			
1. Employer ID Number (if applicable):		2. Canada Revenue Agency Business Number (first 9 digits are mandatory for Canadian businesses):	
3. Business Legal Name:		4. Business Operating Name:	
5. Business Mailing Address:			
6. City:	7. Province/State:	8. Country:	9. Postal Code:
10. Business Telephone Number:		11. Business Address (if different than mailing address):	
12. City:	13. Province/State:	14. Country:	15. Postal Code:
16. Type of business (select all that apply): <input type="checkbox"/> incorporated/limited <input type="checkbox"/> partnership <input type="checkbox"/> sole proprietor <input type="checkbox"/> other, specify _____			
17. Is the business a franchise? <input type="checkbox"/> No <input type="checkbox"/> Yes If yes, is the corporate head office aware of this application for temporary foreign workers (TFW)? <input type="checkbox"/> Yes <input type="checkbox"/> No Provide the name of the corporation: _____			
18. Website Address:		19. Date Business Started: (YYYY-MM-DD)	
20. Describe the principal business activity:			

21. Primary Contact Name: First Middle Last			22. Job Title:		
23. Contact Phone Number: Ext.:		24. Fax Number:		25. E-mail:	
26. Preferred Official Language of Correspondence: <input type="checkbox"/> English <input type="checkbox"/> French					
THIRD-PARTY, RECRUITER OR EMPLOYMENT AGENCY INFORMATION					
1. Are you using the services of a third-party, recruiter or employment agency for the purpose of hiring a TFW? <input type="checkbox"/> No <input type="checkbox"/> Yes If yes, complete the boxes on the right			2. Name of third-party, recruiter or employment agency:		
Note: In some provinces/territories it is mandatory to be registered in order to recruit TFWs on behalf of an employer. For more information visit: www.esdc.gc.ca/eng/jobs/foreign_workers/higher_skilled/index.shtml			3. Registration, license or certificate number:		
4. Are you appointing a third-party to represent you in completing this application form or to provide advice in an immigration process? <input type="checkbox"/> No <input type="checkbox"/> Yes If yes, complete Schedule A - Third-party representative			5. Name of third-party representative:		
6. A number of provinces/territories prohibit the charging of recruitment fees to TFWs for the purpose of securing a job offer. Have you the employer or any other third-party in connection to this job offer received payment from the TFWs to secure this offer of employment? <input type="checkbox"/> Yes <input type="checkbox"/> No					
BUSINESS DETAILS					
1. Number of employees currently employed nationally under this Canada Revenue Agency Business number (e.g. 5 franchises are covered by the business number and there are a total of 100 employees):					
2. Total number of employees currently employed at the work location specified on this form:					
3. Total number of Canadian/permanent resident employees at the work location specified on this form:					
4. Total number of employees (including Canadians/permanent residents and TFWs) working in this occupation at this work location:					
5. Total number of TFWs (as the result of receiving a positive LMIA) at the work location specified on this form:					
6. Did you employ a TFW (as the result of receiving a positive LMIA) in the last two years, prior to December 31, 2013? <input type="checkbox"/> Yes <input type="checkbox"/> No If YES – did you provide all TFWs employed by you in the last two years with wages, working conditions and employment in an occupation that were substantially the same as those that were described in the offer(s) of employment (and confirmed in the LMIA letter(s) and annexe(s))? <input type="checkbox"/> Yes <input type="checkbox"/> No					
7. Have you applied for and received a positive LMIA on or after December 31, 2013, and employed a TFW in that position? <input type="checkbox"/> Yes <input type="checkbox"/> No If YES – did you provide all TFWs employed by you, on LMIAs received on or after December 31, 2013, with employment in the same occupation as described in the offer(s) of employment (and confirmed in the LMIA letter(s) and annexe(s)) and with substantially the same wages and working conditions - but not less favourable than- those set out in that offer(s) of employment (and confirmed in the LMIA letter(s) and annexe(s))? <input type="checkbox"/> Yes <input type="checkbox"/> No Note: Employers should be aware that with recent changes to the Immigration and Refugee Protection Regulations, the look back period has changed from 2 to 6 years. However, this change is not retroactive and, therefore will not be fully implemented until January 2020.					
8. Have you had an LMIA revoked within the previous 2 years from the date you submitted this application? <input type="checkbox"/> No <input type="checkbox"/> Yes If yes, was the LMIA revoked because you had provided false, misleading or inaccurate information in the context of a request for an opinion. <input type="checkbox"/> No <input type="checkbox"/> Yes If yes, please provide the following details regarding this revocation: Date (YYYY-MM-DD): System File Number: If the public policy considerations that justified the revocation are no longer relevant, please provide a detailed explanation:					

<p>9. Were any employees laid off in the past 12 months?</p> <p><input type="checkbox"/> No</p> <p><input type="checkbox"/> Yes If yes, how many Canadians/permanent residents? _____ How many TFWs? _____</p> <p>Reason(s) for layoff(s) and occupations affected: _____</p>														
<p>10. Does your business receive support through Employment and Social Development Canada's Work-Sharing program?</p> <p><input type="checkbox"/> No</p> <p><input type="checkbox"/> Yes If yes, provide details: _____</p>														
<p>JOB OFFER INFORMATION</p> <p>If you are requesting an LMIA to fill multiple jobs for the identical position/occupation, provide the job offer information only once. However, if there are multiple jobs for different positions/occupations, use a separate application form for each unique position/occupation.</p>														
<p>1. Are you applying for an LMIA to hire a TFW in a Caregiver position? <input type="checkbox"/> No <input type="checkbox"/> Yes</p> <p>If yes, employers hiring:</p> <ul style="list-style-type: none"> • an In-home Caregiver must complete this form and Schedule G - In-Home Caregiving Occupations. • a Caregiver to work in a Health Institution must complete this form. 														
<p>2. Job Title: _____</p>		<p>3. Number of TFWs requested for this job offer (same wage, job description, location, etc.): _____</p>												
<p>4. Expected employment duration:</p> <p>_____ Days _____ weeks _____ months _____ years</p>		<p>5. Expected employment start date (YYYY-MM-DD): _____</p>												
<p>6. Provide exact location where the TFW will be working (number and street address): _____</p>														
<p>7. City: _____</p>	<p>8. Province: _____</p>	<p>9. Postal Code: _____</p>												
<p>10. Describe the main duties of the job: _____</p>														
<p>11. Minimum education requirements of the job:</p> <table style="width: 100%; border: none;"> <tr> <td><input type="checkbox"/> Doctorate/PhD</td> <td><input type="checkbox"/> Doctor of Medicine</td> <td><input type="checkbox"/> Master's degree</td> </tr> <tr> <td><input type="checkbox"/> Bachelor's degree</td> <td><input type="checkbox"/> College level diploma/certificate</td> <td><input type="checkbox"/> Apprenticeship diploma/certificate</td> </tr> <tr> <td><input type="checkbox"/> Trade diploma/certificate</td> <td><input type="checkbox"/> Secondary school</td> <td><input type="checkbox"/> Vocational school diploma/certificate</td> </tr> <tr> <td colspan="3"><input type="checkbox"/> No formal education requirement</td> </tr> </table> <p>Additional Information: _____</p>			<input type="checkbox"/> Doctorate/PhD	<input type="checkbox"/> Doctor of Medicine	<input type="checkbox"/> Master's degree	<input type="checkbox"/> Bachelor's degree	<input type="checkbox"/> College level diploma/certificate	<input type="checkbox"/> Apprenticeship diploma/certificate	<input type="checkbox"/> Trade diploma/certificate	<input type="checkbox"/> Secondary school	<input type="checkbox"/> Vocational school diploma/certificate	<input type="checkbox"/> No formal education requirement		
<input type="checkbox"/> Doctorate/PhD	<input type="checkbox"/> Doctor of Medicine	<input type="checkbox"/> Master's degree												
<input type="checkbox"/> Bachelor's degree	<input type="checkbox"/> College level diploma/certificate	<input type="checkbox"/> Apprenticeship diploma/certificate												
<input type="checkbox"/> Trade diploma/certificate	<input type="checkbox"/> Secondary school	<input type="checkbox"/> Vocational school diploma/certificate												
<input type="checkbox"/> No formal education requirement														
<p>12. Minimum experience/skills requirements of the job: (include years of experience and/or occupational designations such as CA, CMA, CGA, R.N., P. Eng) _____</p>														
<p>13. Indicate the language requirement stated in the offer of employment:</p> <p><input type="checkbox"/> The offer of employment does not require the ability to communicate in any specific language.</p> <p><input type="checkbox"/> The offer of employment requires the ability to communicate orally in:</p> <p style="padding-left: 40px;"> <input type="checkbox"/> English <input type="checkbox"/> French <input type="checkbox"/> English or French <input type="checkbox"/> English and French </p> <p><input type="checkbox"/> The offer of employment requires the ability to communicate in writing in:</p> <p style="padding-left: 40px;"> <input type="checkbox"/> English <input type="checkbox"/> French <input type="checkbox"/> English or French <input type="checkbox"/> English and French </p>														

<input type="checkbox"/> The offer of employment requires the ability to communicate in a language other than English or French. If this option is selected, identify the specific language needed and clearly describe why this is a bona fide employment requirement for performing the duties associated with the employment. If insufficient space, attach a separate signed and dated sheet.															
14. Wage in Canadian dollars and number of work hours. Note: Employers must provide the calculation of an hourly rate. <table style="width: 100%; border: none;"> <tr> <td style="width: 20%; text-align: right;">\$ per hour</td> <td style="width: 20%; text-align: right;">\$ per year</td> <td style="width: 20%;"></td> <td style="width: 20%; text-align: right;">Number of hours per day</td> <td style="width: 20%; text-align: right;">Total number of hours per week</td> <td style="width: 20%; text-align: right;">Total number of hours per month</td> </tr> <tr> <td style="border-bottom: 1px solid black;"></td> <td style="border-bottom: 1px solid black;"></td> <td></td> <td style="border-bottom: 1px solid black;"></td> <td style="border-bottom: 1px solid black;"></td> <td style="border-bottom: 1px solid black;"></td> </tr> </table> Overtime rate of \$ _____ starts after _____ hours of work per week.		\$ per hour	\$ per year		Number of hours per day	Total number of hours per week	Total number of hours per month								
\$ per hour	\$ per year		Number of hours per day	Total number of hours per week	Total number of hours per month										
15. What is the wage range for these employees currently working in this occupation at this work location? Low-wage: \$ _____ /hour High-wage: \$ _____ /hour OR <input type="checkbox"/> there are no employees currently working in this occupation at this work location Note: The wage range should be from the last 2 pay periods that have occurred within the 6 weeks prior to submitting the application.															
16. Vacation (if applicable) Days: _____ (# of business days per year) OR Remuneration: _____ (% of gross salary)															
17. Is the job offer for full-time employment (at least 30 hours of work per week) throughout the duration of employment covered by the LMIA? <input type="checkbox"/> Yes <input type="checkbox"/> No If no, explain.															
18. Is this employment seasonal? <input type="checkbox"/> Yes <input type="checkbox"/> No															
19. Benefits: <input type="checkbox"/> Disability insurance <input type="checkbox"/> Dental insurance <input type="checkbox"/> Pension <input type="checkbox"/> Extended medical insurance (e.g. prescription drugs, paramedical services, medical services and equipment)															
20. Other benefits (specify): <div style="border: 1px solid black; height: 40px;"></div>															
21. Are there any federal/provincial/territorial certification, licensing or registration requirements for this job? <input type="checkbox"/> No <input type="checkbox"/> Yes If yes, what is the name of the certifying/licensing/registering body? <div style="border: 1px solid black; height: 40px;"></div> Will the TFW have all required certification, licensing, or registration prior to entering and starting work in Canada? <input type="checkbox"/> No If no, indicate the anticipated period of time to acquire all of the required qualifications after starting work <div style="display: flex; justify-content: space-between; width: 80%;"> _____ Days: _____ weeks _____ months </div> <input type="checkbox"/> Yes If yes, the TFW must have proof that he/she already has all the required qualifications. Note: Securing the necessary documents to practice in Canada is the employer's and the worker's responsibility. CIC must be satisfied that the skilled workers are capable of performing the employment being offered to them. CIC will check to ensure the skilled workers hold the required certification, or license to practice in a regulated occupation in Canada. If the applicant is not certified or licensed, CIC will assess whether the applicant is likely to qualify for licensing/certification when in Canada.															
22. Is the position part of a union? <input type="checkbox"/> No <input type="checkbox"/> Yes If yes, what is the name of the union and the local?															

<p>Has the union been consulted about the hiring of a TFW?</p> <p><input type="checkbox"/> No If no, explain: _____</p> <p><input type="checkbox"/> Yes If yes, what is the position of the union? Provide details and attach documentation, if available. _____</p>	
<p>23. Have you attempted to recruit Canadians/permanent residents for this job?</p> <p><input type="checkbox"/> No If no, explain: _____</p> <p><input type="checkbox"/> Yes If yes, you must provide proof of recruitment (e.g. copy of advertisements and information to support where, when and for how long the position was advertised). _____</p> <p>In addition, if you advertised on the Job Bank (or the provincial/territorial equivalent), provide the order number: _____</p>	
<p>24. What are the potential benefits to the Canadian labour market for offering this job to a TFW(s)?</p> <p><input type="checkbox"/> Filling a labour shortage <input type="checkbox"/> Development or transfer of skills and knowledge for the benefit of Canadians/permanent residents</p> <p><input type="checkbox"/> Other <input type="checkbox"/> Direct job creation or job retention of Canadians/permanent residents</p> <p>Provide Details: _____</p>	
<p>25. Provide a rationale for the job offer you are making to the TFW(s) and describe how this will meet your employment needs: _____</p>	
<p>26. Do you plan to hire or train Canadians/permanent residents for the position(s) for which you are requesting an LMIA ?</p> <p><input type="checkbox"/> No If no, explain: _____</p> <p><input type="checkbox"/> Yes If yes, provide a brief description of the training plan: _____</p>	
<p>27. Will you provide the temporary foreign worker with suitable and affordable accommodation ?</p> <p><input type="checkbox"/> No, but I will assist by doing the following: _____</p> <p><input type="checkbox"/> Yes If yes, please indicate the rent : CAD\$ _____ <input type="checkbox"/> per week or <input type="checkbox"/> per month</p> <p>and describe the type of accommodation: _____</p> <p><input type="checkbox"/> Not applicable</p>	
<p>SUMMARY OF RESULTS TO MEET MINIMUM RECRUITMENT AND ADVERTISEMENT REQUIREMENT</p> <p>You must provide a brief summary of the results of the activities you conducted to meet the minimum recruitment and advertisement requirements to apply for an opinion.</p>	
<p>1. Number of applications/resumes received from Canadians/permanent residents: _____</p>	<p>2. Number of Canadian/permanent resident applicants interviewed: _____</p>
<p>3. Number of Canadians/permanent residents offered the position: _____</p>	<p>4. Number of Canadians/permanent residents hired: _____</p>

<p>5. Number of job offers declined by Canadian/permanent resident applicants:</p>	<p>6. Number of Canadian/permanent resident applicants who were not qualified for the job:</p>																												
<p>7. For each unsuitable Canadian/permanent resident applicant, provide an explanation as to why the candidate did not meet the requirements of the position, if necessary, attach a separate sheet. However, do not provide the names of the candidates (e.g. applicant #1 – has not completed the apprenticeship program and therefore cannot work as a journeyperson, applicant #2 – (unable to communicate in English to the level required for service in a fast paced environment).</p>																													
<p>TRANSITION TO A CANADIAN WORKFORCE</p>																													
<p>There are 2 possible paths for employers to transition to a Canadian workforce. The path that an employer must follow is determined by the wage being offered to the TFW for the position, in relation to the provincial/territorial median hourly wage, based on Statistics Canada's Labour Force Survey (2014).</p> <p>Exemptions: The requirement to transition to a Canadian workforce is not applicable to employers who are hiring TFWs for:</p> <ul style="list-style-type: none"> • on-farm primary agricultural positions, specifically <ul style="list-style-type: none"> • farm managers/supervisors and specialized livestock workers (NOC 8251, 8252, 8253, 8254 and 8256); and • general farm workers, nursery and greenhouse workers and harvesting labourers (NOC 8431, 8432 and 8611). • caregiver positions in a: <ul style="list-style-type: none"> • private household (NOC 3152, 3233, 3413, 6741 and 6474); and • health care facility (NOC 3152, 3233, 3413 and 6741). • positions where they are submitting an application to exclusively support a TFW's permanent residence under an Express Entry program (the TFW will not be applying for a work permit). • positions in highly mobile industries or occupations when the: <ul style="list-style-type: none"> • workforce regularly crosses inter-jurisdictional boundaries (e.g. provincial, territorial and/or international) as part of the business' ongoing operations or the international mobility-based nature for an occupation; and • position will not be filled after the worker leaves; and • position is for 120 days or less. <p>Note: In exceptional circumstances the position can be for a period of more than 120 days when the entry of TFWs has implications for public health and safety.</p> <p>Employers hiring TFWs in these positions, go to the IMPACTS ON THE CANADIAN LABOUR MARKET section</p>																													
<p>The provincial/territorial median hourly wages are as follows:</p> <table border="1" style="width: 100%; border-collapse: collapse;"> <tr> <td style="width: 33%;">Alberta</td> <td style="width: 33%;">\$25.00</td> <td style="width: 33%;">Nunavut</td> <td style="width: 33%;">\$29.00</td> </tr> <tr> <td>British Columbia</td> <td>\$22.00</td> <td>Ontario</td> <td>\$21.15</td> </tr> <tr> <td>Manitoba</td> <td>\$19.50</td> <td>Prince Edward Island</td> <td>\$17.49</td> </tr> <tr> <td>New Brunswick</td> <td>\$18.00</td> <td>Quebec</td> <td>\$20.00</td> </tr> <tr> <td>Newfoundland and Labrador</td> <td>\$21.12</td> <td>Saskatchewan</td> <td>\$22.00</td> </tr> <tr> <td>Northwest Territories</td> <td>\$30.00</td> <td>Yukon</td> <td>\$27.50</td> </tr> <tr> <td>Nova Scotia</td> <td>\$18.85</td> <td></td> <td></td> </tr> </table>		Alberta	\$25.00	Nunavut	\$29.00	British Columbia	\$22.00	Ontario	\$21.15	Manitoba	\$19.50	Prince Edward Island	\$17.49	New Brunswick	\$18.00	Quebec	\$20.00	Newfoundland and Labrador	\$21.12	Saskatchewan	\$22.00	Northwest Territories	\$30.00	Yukon	\$27.50	Nova Scotia	\$18.85		
Alberta	\$25.00	Nunavut	\$29.00																										
British Columbia	\$22.00	Ontario	\$21.15																										
Manitoba	\$19.50	Prince Edward Island	\$17.49																										
New Brunswick	\$18.00	Quebec	\$20.00																										
Newfoundland and Labrador	\$21.12	Saskatchewan	\$22.00																										
Northwest Territories	\$30.00	Yukon	\$27.50																										
Nova Scotia	\$18.85																												
<p>Is the wage you are offering for the position at or above the provincial/territorial median hourly wage in the province/territory where the job is located?</p> <p><input type="checkbox"/> No If no, complete the following Section A – Cap for Low-wage Positions</p> <p><input type="checkbox"/> Yes If yes, skip to Section B – Transition Plans for High-wage Positions</p>																													
<p>Section A - Cap for the Low-wage Positions</p>																													
<p>Employers hiring TFWs and offering a wage that is below the provincial/territorial median hourly wage will be subject to a maximum 10% cap on the proportion of these low-wage TFWs. The cap will be phased in over the next 2 years to provide employers who use the program with time to transition to a Canadian workforce.</p> <p>Employers that have a low-wage TFW workforce will be subject to an established cap, which is the lesser of their current percentage of TFWs in low-wage positions, or</p> <ul style="list-style-type: none"> • 30% as of June 20, 2014 • 20% as of July 1, 2015; and • 10% as of July 1, 2016. 																													

Exemptions to the Cap Requirement:

There is one exemption to the low-wage cap requirement. Employers should check the box if the following is applicable to their business:

- ☐ The business has fewer than 10 employees nationally, including the position to be staffed with TFWs;

Employers, who are exempt from the Cap requirement, go to the **IMPACTS ON THE CANADIAN LABOUR MARKET** section.

Employers, who are NOT exempt from the Cap requirement must complete **Schedule E - Cap for Low-wage Positions**.

Section B - Transition Plan for High-wage Positions

The Transition Plan is a mandatory requirement for all employers applying to hire TFWs, and are offering a wage that is at or above the provincial/territorial median hourly wage.

Rationale For Possible Exemption:

To be considered for an exemption from having to provide a Transition Plan, the employer must complete this section and provide a justification on how they meet the criteria indicated in the following question. Exemptions will be considered on a case by case basis.

Employers who are NOT exempt from the Transition Plan requirement must complete **Schedule C - Employer Transition Plan**.

1. What are the requirements of the position? Select all of the exemption criteria that apply to the position specified on this LMA.

- ☐ The position has a limited duration which means – the job is time-limited and will no longer exist after the TFW leaves.

The employment duration is:

- ☐ 1 to 120 days (e.g. emergency or warranty work)
☐ more than 120 days to a maximum of 2 years (e.g. non-recurring project-based positions)

- ☐ The position is exempt under the Quebec Facilitated Process

(Note: Under the Facilitated Process, a Transition Plan is only required on the second LMA application for the same occupation.)

2. Provide details:

IMPACTS ON THE CANADIAN LABOUR MARKET

The questions in this section are to be completed by all employers. The response to these questions will assist the Program to determine the impact the employment of temporary foreign workers will have on the Canadian labour market.

For the purpose of the Program:

Offshoring - is the relocation by a company of a business process from Canada to another country. This would include an operational process, such as manufacturing, or supporting processes (e.g. accounting or IT services). More recently, offshoring has been associated with technical and administrative services supporting domestic and global operations from outside Canada.

Outsourcing - is the contracting out of a Canadian business process to a foreign or Canadian third party organization resulting in the entry of Temporary Foreign Workers into Canada.

1. Will the entry of these TFWs lead to job losses, now or in the foreseeable future, for Canadians/permanent residents as a result of lay-offs, outsourcing, offshoring or other factors related to utilizing TFWs?

- ☐ No

- ☐ Yes If yes, provide a summary of the impact of hiring these TFWs, on your workforce (e.g. lay-offs, relocations) and the Canadian workforce more generally

<p>2. Is this job offer related to an activity, contract or a subcontract that will facilitate outsourcing or offshoring?</p> <p><input type="checkbox"/> No If no, go to the next section</p> <p><input type="checkbox"/> Yes If yes, you must:</p> <ul style="list-style-type: none"> - complete the following questions (a to c) and - have each employer with whom you have a contractual arrangement to provide services, complete a separate Schedule B – Impacts on the Canadian Labour Market. 	
<p>a.) Provide a summary of the contractual arrangement between the employer of record and the company receiving services including (but not limited to) information on: the purpose and scope of the project, the project timelines, the expertise required, and the number of Canadians and permanent residents working on the project.</p>	
<p>b.) Provide details on how Canadians/permanent residents with whom you have a contractual arrangement for services will be positively and/or negatively affected by this arrangement? (e.g. lay-offs, relocation, displacement, promotions, restructuring, transfer of skills and/or knowledge).</p>	
<p>c.) As part of this contractual arrangement, have you hired any foreign nationals through any work permit-exempt or Labour Market Impact Assessment-exempt processing stream?</p> <p><input type="checkbox"/> No</p> <p><input type="checkbox"/> Yes If yes, complete the following two questions (i) and (ii.)</p>	
<p>c-i) Provide details on efforts in the past two years to hire and/or train Canadians/permanent residents for positions where a foreign national has entered under a work permit-exemption or Labour Market Impact Assessment-exemption.</p>	
<p>c-ii) Provide a summary of the impact of hiring these foreign nationals on Canadians/permanent resident workers within the company receiving services under this contractual arrangement (e.g. lay-offs, relocation).</p>	
<p>FILM AND ENTERTAINMENT REQUEST ONLY</p>	
1. Name of the production:	2. Total number of people involved in the production:
3. Type of Production:	
<p>4. A copy of the contract between the employer and the foreign entertainer must be included with this application form, except for film and TV requests. Is the contract included with application? <input type="checkbox"/> Yes <input type="checkbox"/> No If no, please explain:</p>	

TEMPORARY FOREIGN WORKER INFORMATION	
<p>If you are hiring more than one TFW, use separate sheets to identify each worker coming to work for you in Canada. If the TFW information is not available, leave this section blank.</p> <p>Note: After the positive LMIA letter and annexes have been issued, six months will be allocated to the:</p> <ul style="list-style-type: none"> • employer to provide ESDC/Service Canada with the names of the TFWs; and • TFWs to submit an application for a work permit to Citizenship and Immigration Canada. 	
1. Surname (family name) as shown on the passport:	2. Given name(s) as shown on the passport:
3. Gender: <input type="checkbox"/> Male <input type="checkbox"/> Female	4. Date of Birth (YYYY-MM-DD):
5. Location of residence outside Canada: City: _____ Country: _____	6. Citizenship(s):
<p>7. If the TFW is currently in Canada, please indicate his/her location (city and province) and immigration status:</p> <p>City: _____ Province: _____</p> <p>Status: <input type="checkbox"/> Temporary Foreign Worker (Foreign Live-in Caregiver) <input type="checkbox"/> Temporary Foreign Worker <input type="checkbox"/> Visitor <input type="checkbox"/> Student <input type="checkbox"/> Refugee Claimant</p>	

DECLARATION OF EMPLOYER	
<p>I am an unincorporated employer, sole proprietor or partnership. <input type="checkbox"/> Yes <input type="checkbox"/> No</p>	
<p>If you answered "YES" to the above:</p>	
<p>I understand that some provinces and territories operate, pursuant to agreements with the federal Department of Citizenship and Immigration, Provincial Nominee Programs. I hereby consent to ESDC providing the personal information contained in this request for a Labour Market Impact Assessment to the provincial/territorial government(s) of the province(s) or territory(ies) where I carry on business to be used by the province(s) or territory(ies) for the administration of their Provincial Nominee Programs.</p>	<p><input type="checkbox"/> Yes <input type="checkbox"/> No</p>
<p>Employers must check each box to declare that they comply (or will comply) with the statements below :</p>	
<p><input type="checkbox"/> I certify that I am an employer who does not, on a regular basis, offer strip tease, erotic dance, escort services or erotic massages. I understand that any LMIA application from an employer, who offers these services on a regular basis, will not be processed.</p>	
<p><input type="checkbox"/> I certify that I am actively engaged in the business in respect of which the offer of employment is made and understand that I must remain so during the period of employment for which the work permit is issued to the TFW(s).</p>	
<p><input type="checkbox"/> I certify that the offer is consistent with my reasonable employment needs</p>	
<p><input type="checkbox"/> I certify that I am reasonably able to fulfill the terms of the employment offer</p>	
<p><input type="checkbox"/> I certify that I am compliant with, and will comply with the federal/provincial/territorial laws that regulate employment and the recruitment of employees, in the province/territory in which it is intended that the TFWs work and, if applicable, with the terms and conditions of any collective agreement.</p>	
<p><input type="checkbox"/> I certify that all recruitment done, or that may be done on my behalf, by a third-party was, and will be, in compliance with federal/provincial/territorial laws governing recruitment. I acknowledge and understand that I will be held accountable for the actions of any third-party recruiting TFWs on my behalf.</p>	
<p><input type="checkbox"/> I certify that I am aware of the published recruitment and advertising requirements of the Temporary Foreign Worker Program. I am, and will continue to be, compliant with these requirements and I can provide proof upon request.</p>	
<p><input type="checkbox"/> I certify that the employment of a foreign worker will not adversely affect the settlement of any labour dispute in progress or the employment of any person involved in the dispute, should there be an ongoing or pending labour dispute at my business. I will inform Service Canada in the case one should develop.</p>	

- ☐ I will comply with the prevailing wage requirements and I agree to review and adjust, when applicable, the TFWs wages, at least annually, to ensure he/she continues to receive the prevailing wage for the occupation and region where he/she is employed.
- ☐ I certify that I will make reasonable efforts to provide a workplace that is free of abuse which includes physical, sexual, psychological or financial abuse.
- ☐ I certify that I will provide the TFWs with employment in the same occupation as that set out in the TFWs offer of employment and with wages and working conditions that are substantially the same as — but not less favourable than — those set out in the LMIA letter and annex A.
- ☐ I agree that I will not recover any costs, directly or indirectly, associated with seeking an LMIA from any TFW(s).
- ☐ I acknowledge and understand that for a period of six years from the first day of employment of the TFW(s), I may be subject to an inspection and I will retain any documents that relate to the LMIA application and the terms and conditions of the LMIA letter and annexes.
- ☐ If required, I will give all reasonable assistance to the officer conducting the inspection. I will attend interviews and on-site inspections, answer questions, provide information and documentation that relate to the conditions I have agreed to, pertaining to the LMIA letter and annexes.
- ☐ I understand that should an on-site inspection be required for verification of compliance with the conditions stated on the LMIA letter and annexes, the inspections may take place at any premises or location where the TFW(s) perform(s) work and any premises or place that the employer has provided to the TFW(s) as accommodations. In the case of private dwellings, employer consent or a warrant will be required.
- ☐ I will provide Service Canada with the names of the TFW(s) I intend to employ within six months from the date on the LMIA letter.
- ☐ I declare that the employment of the TFW(s) is likely to have a positive or neutral effect on the Canadian labour market and will not lead to job loss or reduction in work hours for any Canadian or permanent resident during the period of employment for which the work permit is issued.
- ☐ I agree to pay the total fee indicated in the Labour Market Impact Assessment Application - Processing Fee Payment section, either by credit card or certified cheque/money order. I also acknowledge that if I do not submit my payment, my LMIA application will not be processed. This attestation and the requirement to pay the processing fee are NOT applicable to employers who meet the definition of on-farm primary agriculture and are hiring TFWs in the following NOC codes 8251, 8252, 8253, 8254, 8256, 8431, 8432 and 8611.

Employers hiring TFWs in low-wage positions must check the following boxes to declare that they comply (or will comply) with the statements below.

- ☐ I have signed and enclosed a copy of the employment contract related to the job offer referred to in this LMIA application. I certify that this offer of employment meets all Program requirements. The terms and conditions in the offer, including the wages, working conditions, job duties and any benefits are (or will be adjusted to be) the same as those that will be described in the LMIA letter and annexes.
- ☐ I will retain a copy of the contract, related to the offer of employment, signed by all parties. I understand and agree that ESDC may request a copy during an employer compliance review or an inspection.
- ☐ I will pay all transportation costs for the TFW(s) to travel from their country of residence to the location of work in Canada and for the return transportation to their country of residence. If the TFW is already in Canada, I will pay all transportation costs from their residence in Canada to the location of work in Canada, and for the return transportation to their country of residence. I will not recover, directly or indirectly, any of these costs from any TFW(s).
- ☐ I will arrange and pay for private health insurance for the TFW(s), which is similar to provincial/territorial health care coverage, until he/she is eligible for provincial/territorial health care insurance coverage (where applicable) and will not recover these costs from the TFW.
- ☐ I am in good standing with the applicable workers' compensation program and I will register the TFW(s) under the appropriate provincial/territorial workers' compensation/workplace safety insurance plans, where available, or purchase, on-the-job injury or illness insurance that provides the TFW(s) with protection similar to the one offered by the applicable provincial/territorial law. I will not recover these costs from the TFW.

Important:

Employers must immediately inform Service Canada of any changes related to the foreign worker's terms and conditions of employment as described in the positive LMIA letter and annex. If Service Canada accepts the employer's changes to the original LMIA, the employers' file will be updated accordingly.

In accordance with the provisions of the Immigration and Refugee Protection Regulations, ESDC may conduct an inspection to verify the employer's compliance with the conditions set out in the positive LMIA letter and annexes. As a result, this inspection could include a review of the employer's file and if Service Canada does not have a copy of the changes, the employer will be held accountable for the information that is on file.

SIGNATURE OF EMPLOYER	
<p>The individual signing this form must have authority for either the hiring or financial decisions of the organization (e.g. owner, franchisee, general manager, or senior executive – such as VP Human Resources). For In-home Caregiver positions, employers must be a parent, legal guardian, be the recipient of care or have a valid power of attorney, etc.</p>	
<p>I have read and I understand the Personal Information Collection Statement found at the beginning of this application. I declare that the information provided in this Labour Market Impact Assessment is true, accurate and complete.</p>	
Signature of Employer	Printed Name of Employer
Title of Employer	Date (YYYY-MM-DD)
<p>A person, who contravenes a provision set out under sections 126 or 127 of the Immigration and Refugee Protection Act (misrepresentation), could be liable to a fine or to imprisonment, or to both. Also, providing inaccurate information, in the context of this application, may lead to an administrative penalty such as being ineligible to access the Program for a period of two years.</p>	

DOCUMENTATION REQUIRED
New employers hiring a TFW must always submit one document which supports their active engagement in the business. Returning applicants to the Program are not required to re-submit any documentation. However, ESDC/Service Canada may request employers submit additional documents when they are applying for a new LMIA. Employers, who provide documents that are not requested, may find that this slows down the processing of their application. If a required document is not attached, please explain.
Proof of recruitment (e.g. copy of advertisement and information to support where, when and for how long the position was advertised)
Business registration or legal incorporation documents (if first LMIA application) Does not apply to employers of In-home Caregivers.
Municipal/provincial/territorial business license (where applicable and if first LMIA application) Does not apply to employers of In-home Caregivers.
Canada Revenue Agency: <ul style="list-style-type: none"> T2 Schedule 100 Balance Sheet Information (for corporations only – 2 most recent returns filed) T2 Schedule 125 Income Statement Information (for corporations only – 2 most recent returns filed) Only required if this is the employer's first LMIA application. Does not apply to film and entertainment or employers of In-home caregivers.
Attestation by a lawyer, notary public or chartered accountant confirming that the business exists and the main activity of the business. (for sole proprietorship/partnership)
Letter from a legal business confirming the existence of a contract for a good and/or service with the employer applying for an LMIA
Provincial/Territorial workplace safety and insurance (e.g. workers compensation board) clearance letter/certificate (if applicable)
Commercial lease agreement (where applicable and if first LMIA) Does not apply to employers of In-home Caregivers.
Film and Entertainment – copy of employment contract (except film and TV)
Provincial documentation requirements (for the provinces noted below): ALBERTA - Employment Agency Business Licence (<i>Alberta's Fair Trading Act</i>) if applicable BRITISH COLUMBIA - Employment Agency License (<i>British Columbia's Employment Standards Act</i>) if applicable MANITOBA - Certificate of Registration (<i>Manitoba's Worker Recruitment and Protection Act</i>) NOVA SCOTIA - Employer Registration Certificate (<i>Labour Standards Code</i>) SASKATCHEWAN - Employer Registration Certificate (<i>The Foreign Worker Recruitment and Immigration Services Act</i>) (no documentation required, however employers must be registered). Note: In some cases the province may not provide a physical document but rather post the names of registered/certified employers on a website. Send Application and all Supporting Documentation: Employers must sign, and send the completed application and all required documentation to the Service Canada Centre responsible for processing applications in their area. A list of LMIA Processing centres is available on the ESDC website: www.esdc.gc.ca/eng/jobs/foreign_workers/scc.shtml Employers hiring In-home caregivers must send the completed application and all required documentation to the Service Canada Centre, in Ontario, responsible for processing In-home caregiver applications: www.esdc.gc.ca/eng/jobs/foreign_workers/scc.shtml#icp All employers requiring assistance can contact: 1-800-367-5693 (toll-free) from within Canada and the United States 506-546-7569 from outside Canada and the United States Note: A complete application means that employers have: <ul style="list-style-type: none"> filled out all of the fields in all of the necessary forms; included all of the required documentation; signed the forms where required; and submitted the fee payment with the application, if applicable If an application is submitted and it is not complete, Service Canada staff will inform the employer that the application will not be processed. Incomplete applications and supporting documents submitted with the application will not be retained or returned to the employer. As a result, employers are advised to submit copies, not original documents.

**Please complete the Labour Market Impact Assessment - Processing Fee
Payment Form Printed on next page**



Employment and Social Development Canada
Emploi et Développement social Canada

PROTECTED WHEN COMPLETED - B

For office use only

LABOUR MARKET IMPACT ASSESSMENT – PROCESSING FEE PAYMENT

Employers must pay a processing fee for each position requested, except applications that involve on-farm primary agriculture occupations such as farm managers/supervisors and specialized livestock workers and general farm workers, nursery and greenhouse workers and harvesting labourers (specifically NOC codes 8251, 8252, 8253, 8254, 8256, 8431, 8432 and 8611), and those solely to support a foreign national's immigration application.

The total processing fee, where applicable, must be paid before the employer's LMIA application can be processed.

Step 1 – Complete employer information section:

Employer Business Name:	
Canada Revenue Agency Business Number: (First 9 digits are mandatory for Canadian employers)	

Step 2 – Calculate total labour market impact assessment processing fee in Canadian dollars:

Number of positions requested _____ X \$1,000 = TOTAL processing fee payment of \$ CAD _____

Step 3 – Select method of payment:

- ☐ Certified cheque or money order (postal or bank) made payable to the Receiver General for Canada
- ☐ Credit card (Visa, MasterCard, American Express)

For payment by credit card, complete and sign this section

CREDIT CARD INFORMATION AND PAYMENT AUTHORIZATION			
Name of cardholder (as it appears on the credit card):		Employer primary contact name:	
Credit card type: <input type="checkbox"/> Visa <input type="checkbox"/> MasterCard <input type="checkbox"/> American Express		Credit card number:	Expiry date: MM YYYY
Enter the card security/card verification value code (CVV) (a three or four digit number found on the back or front of the credit card): _____			
AUTHORIZATION:			
I authorize ESDC/Service Canada in the name of the Receiver General for Canada to charge _____ \$ CAD to my credit card. This is permission for a single transaction, and does not provide authorization for any additional charges.			
Signature of cardholder:		Date: YYYY MM DD	

Send this form to Service Canada only

Note:

Refunds will only be provided if a fee was collected in error (e.g. an incorrect fee amount was processed). There will not be refunds in the event of a negative labour market impact assessment since the fee covers the process to assess an application and not the outcome.

Annex E: Appointment of a 3rd Party Representative (for LMIA Application)



Employment and
Social Development Canada

Emploi et
Développement social Canada

PROTECTED WHEN COMPLETED - B

SCHEDULE A APPOINTMENT OF A THIRD-PARTY REPRESENTATIVE

Employers should visit the Temporary Foreign Worker Program website at www.esdc.gc.ca/eng/jobs/foreign_workers/index.shtml to verify that the Program is accepting applications for the specific occupation or sector for which they wish to hire the temporary foreign worker (TFW) and to determine if they are eligible to participate in the Program.

Personal Information Collection Statement

The information you provide on this form is collected by Employment and Social Development Canada (ESDC) under the authority of the *Immigration and Refugee Protection Act (IRPA)* and *Immigration and Refugee Protection Regulations (IRPR)*, for the purpose of providing a Labour Market Impact Assessment (LMIA) in accordance with these statutes. Completion is voluntary; however, failure to complete this form will result in your LMIA application not being processed.

The information you provide may be shared with Citizenship and Immigration Canada (CIC) for the administration and enforcement of the IRPA and IRPR as permitted by the *Department of Employment and Social Development Act (DESD Act)*, and may be accessed by the Canada Border Services Agency (CBSA) for the purpose of issuing work permits at Ports of Entry. ESDC may also provide information to CBSA in order for that agency to investigate and enforce the IRPA and IRPR in relation to an LMIA.

The information may also be shared with provincial/territorial governments for the purpose of administration and enforcement of provincial/territorial legislation including employment standards and occupational health and safety legislation, as permitted by the DESD Act. The information may also be used by ESDC for inspections, policy analysis, research and evaluation in relation to the entry and hiring of TFWs to Canada or the IRPA.

The information you provide is administered under Part 4 of the DESD Act and the *Privacy Act*. You have the right to access and request correction of your personal information, which is described in Personal Information Bank PPJ 440 and PPJ 171 of Info Source. Instructions for making formal requests are outlined in the Info Source publication available online at infosource.gc.ca.

A person, who contravenes a provision set out under sections 126 or 127 of the *Immigration and Refugee Protection Act* (misrepresentation), could be liable to a fine or to imprisonment, or to both. Also, providing inaccurate information, in the context of this application, may lead to an administrative penalty such as being ineligible to access the Program for a period of two years.

For the purpose of a labour market impact assessment application, when appointing a third-party representative all employers MUST complete and submit this form. According to subsection 91(2) of the *Immigration and Refugee Protection Act (IRPA)*, Employment and Social Development Canada (ESDC) and Citizenship and Immigration Canada (CIC) will only conduct business with authorized representatives. The types of authorized representatives that can be used by employers are listed on CIC's website at: www.cic.gc.ca.

THIRD-PARTY BUSINESS INFORMATION			
1. Business Operating Name of Third-Party		2. Canada Revenue Agency Business Number <i>(first 3 digits are mandatory for Canadian businesses)</i>	
3. Legal Name		4. Third-party ID number (if applicable)	
5. Mailing Address			
6. City	7. Province/State	8. Country	9. Postal/Zip Code
10. Business Address (if different from mailing address)			
11. City	12. Province/State	13. Country	14. Postal/Zip Code
15. Describe the main business activity:			

THIRD-PARTY CONTACT INFORMATION (Authorized representative acting on behalf of the employer)			
1. First Name		Middle Name	
Last Name		2. Job title	
3. Telephone Number		Ext:	
4. Fax Number		5. E-mail Address	
6. Business Legal Name		7. Business Operating Name as stated on the LVA application	
8. Preferred Official Language of Correspondence		<input type="checkbox"/> English <input type="checkbox"/> French	
9. Indicate which one of the following applies to the third-party representative: The representative is UNPAID and is: <input type="checkbox"/> a family member or a friend <input type="checkbox"/> a member of a non-governmental or a religious organization <input type="checkbox"/> a member in good standing of the Immigration Consultants of Canada Regulatory Council (ICCRC) a provincial or territorial law society or the Chambre des notaires du Québec <input type="checkbox"/> other (please describe):			
10. The representative is has been, or will be PAID and is a member in good standing of: <input type="checkbox"/> the Immigration Consultants of Canada Regulatory Council (ICCRC) MEMBERSHIP ID: _____ <input type="checkbox"/> a provincial or territorial law society PROVINCE/TERRITORY: _____ MEMBERSHIP ID: _____ <input type="checkbox"/> the Chambre des notaires du Québec MEMBERSHIP ID: _____ <input type="checkbox"/> other (please describe):			
DECLARATION OF THE THIRD-PARTY REPRESENTATIVE			
I, hereby, declare that the above information is true, accurate and complete.			
Signature of the Third-Party Representative		Printed name of the Third-Party Representative	
		Date (YYYY-MM-DD)	

DECLARATION OF EMPLOYER		
FOR THE PURPOSE OF THIS LABOUR MARKET IMPACT ASSESSMENT APPLICATION:		
_____		located at
(Name of employer)		

(Complete employer business address)		
Telephone Number: _____	Fax number: _____	
and _____		
located at		
(Name of employer number 2, if applicable)		

(complete employer address of employer number 2, if applicable)		
Telephone Number: _____	Fax number: _____	
I hereby appoint the third-party indicated on this form as my representative to act on my behalf in order to obtain a Labour Market Impact Assessment opinion from ESDC/Service Canada.		

(Name of the foreign worker to whom the offer of employment has been made or is anticipated to be made)		
I hereby agree to ratify and confirm all that my third-party representative shall do or cause to be done by virtue of this appointment.		
This appointment shall remain in full force and effect only for the processing of this application, unless due notice in writing of its revocation has been given to ESDC/Service Canada.		
Signature of employer _____	Printed name of employer _____	Date (YYYY-MM-DD) _____
Signature of employer number 2 (if applicable) _____	Printed name of employer number 2 _____	Date (YYYY-MM-DD) _____
Signature of witness _____	Printed name of witness _____	Date (YYYY-MM-DD) _____

Annex F: Work Permit Application (Form IMM 1295)



Citizenship and Immigration Canada
Citoyenneté et Immigration Canada

PROTECTED WHEN COMPLETED - B

PAGE 1 OF 4

APPLICATION FOR WORK PERMIT MADE OUTSIDE OF CANADA

If you need more space for any section, print out an additional page containing the appropriate section, complete and submit it with your application.

1 UCI	2 I want service in	OFFICE USE ONLY Validation
-------	---------------------	--------------------------------------

PERSONAL DETAILS

1 Full name <small>Family name (as shown on your passport or travel document)</small>	<small>Given name(s) (as shown on your passport or travel document)</small>
2 Have you ever used any other name (e.g. Nickname, maiden name, alias, etc.)? <small>Family name</small>	<small>Given name(s)</small>

3 Sex	4 Date of birth	5 Place of birth
<input type="checkbox"/> Male <input type="checkbox"/> Female	<input type="checkbox"/> YYY <input type="checkbox"/> MM <input type="checkbox"/> DD	<input type="checkbox"/> City/Town <input type="checkbox"/> Country

6 Citizenship	
---------------	--

7 Current country of residence:				
Country	Status	Other	From	To
			<input type="checkbox"/> YES <input type="checkbox"/> NO	<input type="checkbox"/> YES <input type="checkbox"/> NO

8 Previous countries of residence: During the past five years have you lived in any country other than your country of citizenship or your current country of residence indicated above for more than six months?				
Country	Status	Other	From	To
			<input type="checkbox"/> YES <input type="checkbox"/> NO	<input type="checkbox"/> YES <input type="checkbox"/> NO

9 Country where applying: (Same as current country of residence?)				
Country	Status	Other	From	To
			<input type="checkbox"/> YES <input type="checkbox"/> NO	<input type="checkbox"/> YES <input type="checkbox"/> NO

10 a) Your current marital status	b) If you are married or in a common-law relationship, provide the date on which you were married or entered into the common-law relationship	Date
<input type="checkbox"/> Single <input type="checkbox"/> Married <input type="checkbox"/> Common-law		<input type="checkbox"/> YES <input type="checkbox"/> NO

c) Provide the name of your current Spouse/Common-law partner <small>Family name</small>	<small>Given name(s)</small>
---	------------------------------

FOR OFFICE USE ONLY - DO NOT WRITE IN THIS SPACE

IMM 1295 (06/2016)

APPLICATION FOR WORK PERMIT MADE OUTSIDE OF CANADA

This form is made available by Citizenship and Immigration Canada and is not to be sold to applicants.

(DISPONIBLE EN FRANÇAIS - IMM 1295 F)

Canada

PAGE 3 of 4

Applicant Name		Date of Birth	
----------------	--	---------------	--

PERSONAL DETAILS (CONTINUED)

11 Have you previously been married or in a common-law relationship? ☐ No ☐ Yes

Provide the following details for your previous Spouse/Common-law Partner

Family name		Given name(s)	
Date of birth	Type of relationship	From	To
YYYY MM DD		YYYY-MM-DD	YYYY-MM-DD

LANGUAGE(S)

1 *1st Native language/Mother tongue

2 *If your native language is not English or French, which language do you use most frequently?

3 *Are you able to communicate in English and/or French?

4 Have you taken a test from a designated testing agency to assess your proficiency in English or French? ☐ No ☐ Yes

PASSPORT

1 *Passport number	2 *Country of issue	3 *Issue date	4 *Expiry date
		YYYY-MM-DD	YYYY-MM-DD

CONTACT INFORMATION

If submitting your application by mail:

- All correspondence will go to the address unless you indicate your email address below.
- Indicating an email address will authorize all correspondence, including file and personal information, to be sent to the email address you specify.
- If you wish to authorize the release of information from your application to a representative, indicate their email and mailing addresses in this section and on the IV 5547F form.

1 Current mailing address

PO Box	Apartment	Street no.	*Street name
City/Town	*Country	Province/State	Postal code District

2 Residential address (is this a mailing address?) ☐ No ☐ Yes

Apartment	Street no.	Street name	City/Town
Country	Province/State	Postal code	District

3 Telephone no. ☐ Canadian ☐ Other

Type	Country code No.	Ext.
------	------------------	------

4 Alternate Telephone no. ☐ Canadian ☐ Other

Type	Country code No.	Ext.
------	------------------	------

5 Fax no. ☐ Canadian ☐ Other

Country code No.	Ext.
------------------	------

6 E-mail address

DETAILS OF INTENDED WORK IN CANADA

1 *What type of work permit are you applying for?

2 Details of my prospective employer (attach original offer of employment):

a) Name of Employer (if you are employed by a foreign employer who has been awarded a contract to provide services to a Canadian entity, please identify the foreign employer here)

b) Complete Address of Employer (Canadian or Foreign)

PAGE 4 OF 4

Applicant Name		Date of Birth	
----------------	--	---------------	--

DETAILS OF INTENDED WORK IN CANADA (CONTINUED)

3 Intended location of employment in Canada?			
Province	City/Town	Address	

4 My occupation in Canada will be:		Brief description of duties	
Job title			

5	Duration of expected employment	From	To	6 Labour market opinion (LMO) No
	▶	YYYY-MM-DD	YYYY-MM-DD	

LIVE-IN CAREGIVER PROGRAM

1 Type of care indicate all that apply				2 No. of persons requiring care	
<input type="checkbox"/> Child care	<input type="checkbox"/> Disabled	<input type="checkbox"/> Elderly	<input type="checkbox"/> Other		

EDUCATION

Have you had any post-secondary education (including university, college or apprenticeship training)? ☐ No ☐ Yes

If you answered "yes", give full details of your highest level of post-secondary education.

1	From	Field and level of study	School/Facility name	
	YYYY-MM	YYYY-MM		
	To	City/Town	Country	Province/State
	YYYY-MM	YYYY-MM		

EMPLOYMENT

Give details of your employment for the past 10 years, and/or if you have held any government positions (such as civil servant, judge, police officer, mayor, member of Parliament, hospital administrator).

1	From	Current Activity/Occupation	Company/Employer/Facility name	
	YYYY-MM	YYYY-MM		
	To	City/Town	Country	Province/State
	YYYY-MM	YYYY-MM		

2	From	Previous Activity/Occupation	Company/Employer/Facility name	
	YYYY-MM	YYYY-MM		
	To	City/Town	Country	Province/State
	YYYY-MM	YYYY-MM		

3	From	Previous Activity/Occupation	Company/Employer/Facility name	
	YYYY-MM	YYYY-MM		
	To	City/Town	Country	Province/State
	YYYY-MM	YYYY-MM		

BACKGROUND INFORMATION

You must complete this section if you are 18 years of age or older.

1	<p>a) Within the past two years, have you or a family member ever had tuberculosis of the lungs or been in close contact with a person with tuberculosis? <input type="checkbox"/> No <input type="checkbox"/> Yes</p> <p>b) Do you have any physical or mental disorder that would require social and/or health services, other than medication, during a stay in Canada? <input type="checkbox"/> No <input type="checkbox"/> Yes</p> <p>c) If you answered "yes" to question 1a) or 1b) please provide details and the name of the family member if applicable:</p> <div style="border: 1px solid black; height: 100px; width: 100%;"></div>
---	---

IMM 1295 (06/2014) E
APPLICATION FOR WORK PERMIT MADE OUTSIDE OF CANADA

CITIZENSHIP AND IMMIGRATION - CANADA
CITIZENSHIP ET IMMIGRATION - CANADA

Applicant Name	PAGE 4 OF 4 Date of Birth
BACKGROUND INFORMATION (CONTINUED)	
2 a) Have you ever remained beyond the validity of your status, attended school without authorization or worked without authorization in Canada?	<input type="checkbox"/> No <input type="checkbox"/> Yes
b) Have you ever been refused a visa or permit, denied entry or ordered to leave Canada or any other country?	<input type="checkbox"/> No <input type="checkbox"/> Yes
c) Have you previously applied to enter or remain in Canada?	<input type="checkbox"/> No <input type="checkbox"/> Yes
d) If you answered "yes" to question 2a), 2b), or 2C please provide details: <div style="border: 1px solid black; height: 40px; margin-top: 5px;"></div>	
3	
a) Have you ever committed, been arrested for, been charged with or convicted of any criminal offence in any country?	<input type="checkbox"/> No <input type="checkbox"/> Yes
b) If you answered "yes" to question 3a above, please provide details: <div style="border: 1px solid black; height: 40px; margin-top: 5px;"></div>	
4	
a) Did you serve in any military, militia, or in a defence unit or serve in a security organization or police force (including non-obligatory national service, reserve or volunteer units)?	<input type="checkbox"/> No <input type="checkbox"/> Yes
b) If you answered yes to question 4a), please provide dates of service and countries where you served: <div style="border: 1px solid black; height: 40px; margin-top: 5px;"></div>	
5	
Are you or have you ever been a member or associated with any political party, or other group or organization which has engaged in or advocated violence as a means to achieving a political or religious objective, or which has been associated with criminal activity at any time?	<input type="checkbox"/> No <input type="checkbox"/> Yes
6	
Have you ever witnessed or participated in the ill-treatment of prisoners or civilians, looting or destruction of religious buildings?	<input type="checkbox"/> No <input type="checkbox"/> Yes
If you answered "yes" to any of questions 3 to 6 above, or upon request of a visa officer, you MAY BE REQUIRED to fill out IMM 5252 Schedule 1.	
SIGNATURE	
Citizenship and Immigration Canada (CIC) or an organization at CIC's request, may want to contact you in the future to ask you about any services you received from CIC prior to the application process (such as participation in an information forum), during the application process (including the application process itself as well as orientation or acclimatization services) and services received after arriving in Canada (including settlement, integration and citizenship). CIC will use this information, along with the information provided by other individuals, for research, performance measurement or evaluation purposes. CIC will not use this information to make any decisions about you personally.	
Do you consent to be contacted by CIC or an organization at CIC's request, in the future? (if NE) <input type="checkbox"/> No <input type="checkbox"/> Yes	
I consent to the release to Citizenship and Immigration Canada (CIC) and Canada Border Services Agency (CBSA) of all records and information for the purpose of processing my request that any government authority, including police, judicial and state authorities in all countries in which I have lived may possess about me. This information will be used to evaluate my suitability for admission to Canada or to remain in Canada pursuant to Canadian legislation.	
In order to verify my eligibility for a study permit and my compliance with the conditions of my study permit, I consent to the collection and use of my personal information by CIC, CBSA and, where applicable, my designated learning institution and the provincial/territorial government in which my designated learning institution is located. I further consent to the disclosure of my personal information between CIC and CBSA and, where applicable, between my designated learning institution and CIC, and CIC and the provincial/territorial government, for these purposes. I understand I can withdraw my consent should I not obtain a study permit.	
I declare that I have answered all questions in this application fully and truthfully.	
Signature of Applicant or Parent/Legal Guardian (for a person under 18 years of age): <div style="border: 1px solid black; height: 30px; width: 100%; margin-top: 5px;"></div>	

IMPORTANT NOTE:

 This application must be signed and dated before it is submitted by mail.

Do not forget to include photos, fees if applicable and any other documents required. Review the application guide for more information and verify that you have completed and provided all of the required documents as per the document checklist.

DISCLOSURE

[illegible]

The information you provide to us will be stored on our secure servers (RACOR, INC.) and not RACOR. If you are required to provide electronic identification of your fingerprints, you will act as the RACOR will be storing the RACOR FBI and local entities have a right to protection of any access to your personal information stored in such corresponding RACOR in accordance with the Privacy Policy and the Access to Information Act. Copies of these policies are available at the RACOR website: <http://racorinc.com> and contain the official data retention information. It also enables a mobile device access across a secure

Annex G: Temporary Resident Visa Application (Form IMM 5257)

Citizenship and
Immigration CanadaCroyant et
interne en Canada

PROTECTED WHEN COMPLETED. B

 $\text{H}_2\text{O} + \text{CF}_2$

SCHEDULE 1
APPLICATION FOR TEMPORARY RESIDENT VISA

*The principal applicant, his or her spouse or common-law partner, if applicable, and all dependent children aged 18 years or older listed in the application for temporary residence must complete their own copy of this form.

<input type="checkbox"/> The principal applicant		<input type="checkbox"/> The spouse, common-law partner or dependent child aged 18 years or older of the principal applicant		OFFICE USE ONLY Validated
1 Full name Family name (as shown on your passport or travel document) _____ Given names (as shown on your passport or travel document) _____				
2 Date of birth YY MM DD 3 UOI				
Canada places a high value on bringing those who commit acts of genocide, war crimes or crimes against humanity to justice. Canada was the first country to incorporate the obligations of the Rome Statute into its national laws.				
4 Military Service Did you serve in any military, militia, or civil defence unit or serve in a security organization or police force (including non-obligatory national service, reserve or volunteer units)?				
<input type="checkbox"/> No <input type="checkbox"/> Yes ▶ Give the following details:				
From	To	Location (Place where stationed)	Province	Country
MM	MM			
YY	YY			
YY	YY			
YY	YY			
YY	YY			
Add more rows ▶ +				
5 Have you ever witnessed or participated in the ill treatment of prisoners or civilians, looting or desecration of religious buildings?				
<input type="checkbox"/> No <input type="checkbox"/> Yes ▶ Give the following details:				
From	To	Location	Province	Country
MM	MM			
YY	YY			
YY	YY			
YY	YY			
Details:				
Details:				
Details:				
Add more rows ▶ +				

10/23/06-2014
2014-2015

This form is made available by Citizenship and Immigration Canada and is not to be sold to applicants.
(A-92) D-SECR ELE EN FRANCAIS - IVV 0267 F - Annex 1

Canadă

[illegible]

Annex H: ESDC's Online Fraud Reporting Tool

The following text was taken from ESDC's Online Fraud Reporting Tool which is presented to users in a step-by-step format.

Step 1: How to start

Reporting abuse or misuse for the Temporary Foreign Worker Program

Here are a few things to keep in mind before beginning the online reporting process:

- No feedback will be provided as a result of you submitting information through this process.
- We will not release your identity unless you provide your consent. Sending us your contact information is optional. All leads, whether collected through this tool, or by another method, are privileged and subject to the provisions of the *Privacy Act*.
- ESDC/Service Canada **does not pay** for information received from individuals providing leads on suspected fraud.
- We take all informant leads seriously and apply the same procedures to all information received. However, we encourage you to provide as much detail as possible to assist us in understanding the nature of the allegations.
- Once you have submitted the information through this online process you cannot revoke it.
- All information is reviewed to determine the validity of the allegations and whether further action is necessary. It may not always be appropriate or possible to act on the information immediately, but we will review it and take necessary action.
- Read through the **privacy and security** statements.

Step 2: Review privacy statement

Privacy Notice

Personal information is collected under the authority of the *Privacy Act*.

The information will be used to follow-up on the lead to determine if there is an element of non-compliance with the Temporary Foreign Worker Program legislation, and if applicable, provided to the corresponding compliance program for appropriate enforcement action. Information may also be referred to Citizenship and Immigration Canada (CIC), the Canada Border Service Agency (CBSA) or Employment and Social Development Canada (ESDC) in the event that the lead relates to one of the programs they administer.

The information you provide is voluntary; it will not affect any dealings you may have with the Government of Canada currently or in the future.

You are not obliged to provide us with personal information about yourself. If you choose to provide your personal information, we may contact you to clarify statements or ask for additional information. Any personal information that you provide is protected under the

federal Privacy Act. In addition, Service Canada is legally obliged to take all reasonable measures to protect the identity of informants, information that may indicate the identity of an informant, and even information that might suggest the existence of an informant.

Individuals also have rights of access to, correction of, and protection of their personal information under the Privacy Act: Access to Information.

Security Information

The Government of Canada, Employment and Social Development Canada and Service Canada (SC) are committed to providing visitors with Web sites that are respectful of the diverse needs of Canadians, as well as privacy and copyright laws.

We will ensure that the electronic services we offer continue to meet the strict privacy, confidentiality, and security standards that the legislation requires and that Canadians expect from us.

Service Canada uses corporate firewalls to protect our Web servers from unauthorized access. Any personal information you provide is not stored on these servers; we securely store your personal information on separate computer systems that are not directly accessible from the Internet.

Refer to the Terms and Conditions for the policies and practices that Service Canada adheres to for all online activities.

Step 3: What to send us

The following information will help us determine whether we should undertake an investigation, audit, or other action:

- Location and name of the business or organization name (if applicable)
- Name(s) and contact information of those suspected of abusing or misusing of the program including their address and email, etc. name of those involved (if known)
- Type of abuse you suspect that is relevant to the situation:
 - resident status
 - employee abuse, intimidation, withholding passport or pay cheques, etc.
 - different/wrong occupation
 - displacing Canadians
- Details of your observations
- Relevant documents: have you seen documents?
- Your name and phone number (optional: **you can remain anonymous**); if we require more information, can we contact you?

You may not have all the suggested information, however submitting as much detail as possible will enable us to take the appropriate action to address the issue.

For confidentiality reasons, note that we will not provide you any feedback or give you an update as a result of the information you have submitted. Please be assured that we take all reports of potential misuse or abuse very seriously.

Annex I: CBSA Lead Referral Form (From ESDC Integrity Services Branch)

Protected B
(when completed)

CBSA Lead Referral from SC/ISB		
ALL LEADS MUST BE PROTECTED		
Refer to the informant leads protocol, "Protocol for the Handling of Informant Leads" – Dated January 20, 2014		
Date Referred by SC/ISB to CBSA (M-D-YYYY):		
SharePoint File Reference:		
<input type="checkbox"/> W-T (West and Territories) <input type="checkbox"/> ON (Ontario Region) <input type="checkbox"/> QC (Québec Region) <input type="checkbox"/> ATL (Atlantic Region)	Action Priority and Description <input type="checkbox"/> 1= Urgent <input type="checkbox"/> 2= High <input type="checkbox"/> 3= Medium <input type="checkbox"/> 4= Low	
Employer Legal Name and Address		
Office Name (Operating As)		
TFWP/SC ER ID # (s)		
SF to be reviewed		
Additional Relevant Information (as applicable):		
-Previous reviews for this employer		
Planned Review		
<input type="checkbox"/> For Employer Compliance Reviews (IRPR 203 (1) (e)) WOW (Wages, Occupation and Working Conditions).	<input type="checkbox"/> For Reviews Under Ministerial Instructions (IRPA 30 (1.41/ 1.43)) WOW + Advertising/Recruitment Abuse-free Public Policy Considerations: <input type="checkbox"/> New information becomes available after an LMIA is provided which, if known at the time of the assessment, would have led to a different opinion <input type="checkbox"/> There are reasonable grounds to suspect that the employer or group of employers provided false, misleading or inaccurate information when requesting the LMIA.	<input type="checkbox"/> Inspections (IRPR 209)

Protected B
(when completed)

Allegation (s) / Information
<p>Allegation:</p> <p>ALLEGATION DETAILS:</p>
Informant Contact Details*:
ESDC contact:

Annex J: Information Sharing Agreement Between ESDC and the CBSA

UNCLASSIFIED

INFORMATION SHARING AGREEMENT INVOLVING PERSONAL INFORMATION

Between:

The Department of Employment and Social Development
(Hereinafter referred to as ESDC)

AND

The Canada Border Services Agency
(Hereinafter referred to as the CBSA)

1.0 ENTIRE AGREEMENT

1.1 Information Sharing Agreement (ISA)

The ISA, its Annexes and any amendments made thereto, constitute the entire agreement between the Parties (Agreement).

1.2 Amendment

Unless otherwise stipulated, any amendment to the Agreement is subject to the provisions in the core agreement.

1.3 Definitions

Definitions for terms used in this Agreement are set out in Annex A.

2.0 THE PARTIES

2.1 ESDC

The Department of Employment and Social Development (ESDC) was continued under section 3 of the *Department of Employment and Social Development Act* (DESDA). The Minister of ESDC is responsible for all matters relating to human resources and skills development in Canada or the social development of Canada. The Minister of ESDC is also responsible for the administration and enforcement of certain activities under the *Immigration and Refugee Protection Act* (IRPA) and the *Immigration and Refugee Protection Regulations* (IRPR).

2.2 CBSA

The Canada Border Services Agency (CBSA) was created by Order in Council in 2003. The *Canada Border Services Agency Act* sets out the responsibilities, mandate, powers, duties and functions of the Minister responsible for the Agency and its President. The CBSA is responsible for providing integrated border services that support national security priorities and facilitate the free flow of persons and goods, including animals and plants, which meet all requirements as set out in the CBSA's program legislation (see section 2 of CBSA Act). The CBSA is responsible for

UNCLASSIFIED

administering and enforcing the *Customs Act, Immigration and Refugee Protection Act* (IRPA), and more than 100 other Acts, related regulations, and tariffs.

3.0 PURPOSE OF THE ISA

3.1 This Agreement establishes an administrative framework for the exchange of personal information between the Parties including all aspects of collection, use, disclosure, retention and destruction.

3.2 This Agreement identifies the personal information to be disclosed, the relevant authorities, and the terms and conditions under which that information can be shared between ESDC and the CBSA for the administration and enforcement of their respective responsibilities under the IRPA and IRPR; jointly referred to as IRPA.

3.2.1 The CBSA seeks to obtain information from ESDC for the administration and enforcement of the TFWP and the IRPA. This includes, but may not be limited to, the issuance of work permits, determinations of admissibility and investigation and intelligence gathering activities for the administration and enforcement of IRPA.

3.2.2 ESDC seeks to obtain information from the CBSA for the administration and enforcement of the Temporary Foreign Worker Program (TFWP) and all other activities assigned to ESDC under the IRPA and the IRPR.

4.0 DISCLOSURE BY ESDC TO THE CBSA FOR ADMINISTRATION AND ENFORCEMENT OF THE IMMIGRATION AND REFUGEE PROTECTION ACT

4.1 Authority for ESDC to disclose information

Pursuant to subsection 34(1) of DESDA, ESDC has the authority to make personal information obtained or prepared under its programs (including but not limited to the TFWP) available to the CBSA for the administration or enforcement of the IRPA.

Pursuant to subsection 35(1) of the DESDA, ESDC has the authority to make personal information available to the CBSA for the administration or enforcement of the IRPA, subject to the conditions agreed to herein.

4.2 Authority for the CBSA to collect information

Pursuant to section 4 of the Privacy Act, R.S.C. 1985, c. P-21, the CBSA may only collect personal information that relates directly to an operating program or activity. With respect to this Agreement, the CBSA collects personal information for purposes of the IRPA, including pursuant to Sections 11, 20 and 22 of the IRPA and Part 11 of the IRPR.

UNCLASSIFIED

4.3 Information to be disclosed by ESDC to the CBSA

Where ESDC provides personal and/or employer information to the CBSA, ESDC will search its internal databases, systems and any paper documents and disclose information elements listed in Annex C and Annex D of this Agreement to the extent these are available.

4.4 Secondary disclosure by the CBSA

Subsection 35(2) of DESDA prohibits the CBSA from making available the information obtained from ESDC pursuant to this paragraph to any other person or body unless the Minister of ESD considers it advisable and the information is made available for the same purpose and it is subject to conditions agreed upon by the Minister and the CBSA.

The CBSA hereby undertakes that no subsequent disclosure of the information will be made by the CBSA in a form that could reasonably be expected to identify the individuals to whom it relates unless strictly required by law or permitted pursuant to this Agreement.

5.0 DISCLOSURE BY THE CBSA TO ESDC FOR ADMINISTRATION AND ENFORCEMENT OF THE TEMPORARY FOREIGN WORKER PROGRAM

5.1 Authority for the CBSA to disclose information

Pursuant to paragraph 8(2)(a) of the *Privacy Act*, and under section 209.92 of IRPR, the CBSA has the authority to disclose information related to its programs to the ESDC for the administration or enforcement of the IRPA.

5.2 Authority for ESDC to collect information

Pursuant to section 4 of the *Privacy Act*, R.S.C. 1985, c. P-21, ESDC may only collect personal information that relates directly to an operating program or activity.

Pursuant to sections 30(1.43) of the IRPA and 203 of the IRPR, ESDC is required to provide labour market impact assessments (LMIA) to employers, group of employers or the Department of Citizenship and Immigration (CIC) upon request. In assessing requests for such LMIAs, ESDC is authorized to collect certain personal information.

Section 209 of the IRPR provides the authority for ESDC to conduct inspections and verify an employer's compliance with the conditions outlined in the IRPR. Collection of personal information in the course of these inspections is therefore authorized.

5.3 Information to be disclosed by the CBSA to ESDC

Where the CBSA provides ESDC certain information that will help ESDC identify the personal information sought, the CBSA will search its internal databases, systems and any paper documents and disclose information elements listed in Annex E of this Agreement to the extent these are available.

UNCLASSIFIED

5.4 Secondary disclosure by ESDC

ESDC hereby undertakes that it will not make any secondary disclosure in a form that could reasonably be expected to identify the individual to whom it relates unless strictly required by law.

Section 37 DESDA authorizes ESDC to disclose personal information if the Minister of ESDC considers that it is in the public interest. This is not considered secondary disclosure for purposes of this Agreement.

6.0 ACCESS, CONFIDENTIALITY, USE, DISCLOSURE OF PERSONAL INFORMATION (Disclosed under paragraphs 4 and 5)

6.1 The Parties undertake to use their best efforts to fully maintain and protect the confidentiality of the personal information they receive under this Agreement.

6.2 Only those employees who require the personal information in the course of their employment and duties will have access to it.

6.3 The Parties will not, in respect of any personal information they obtain from each other under this Agreement

- (a) use that information for a purpose other than that for which it was respectively provided to them; and
- (b) disclose that information to any person or body for a purpose other than that for which it was respectively provided to them and as authorized in this Agreement.

6.4 The Parties may use personal information they obtain from each other under this Agreement for a purpose other than that for which it was obtained:

- (a) with the consent of the individual to whom that information relates; or
- (b) if required by legislation.

6.5 The Parties may disclose personal information they obtain from each other under this Agreement to any person or body for any purpose:

- (a) with the consent of the individual to whom that information relates;
- (b) in a form that cannot reasonably be expected to identify the individual to whom that information relates; or
- (c) if required by legislation.

6.6 In the event of a request under the *Access to Information Act* or *Privacy Act* for personal information obtained from another Party, the Parties agree to consult, when required, prior to any disclosure of such information.

UNCLASSIFIED

6.7 The Parties acknowledge that it is an offence under s. 42 DESDA for anyone to knowingly use or make available personal information otherwise than in accordance with this Agreement. An individual found guilty could be subject to a fine of up to \$10,000 or to imprisonment for up to six months, or both. Organizations guilty of the same offence could be subject to a fine of up to \$100,000. This provision also applies to third parties to whom the personal information is disclosed.

7.0 DISCLOSURE TO A THIRD PARTY

7.1 For the purposes of this Agreement, a third party does not include Shared Services Canada, a department of the Government of Canada established under section 4 of the Shared Services Canada Act, S.C. 2012, c. 19, responsible for the provision of information technology (IT) infrastructure services to Canada, that may include e-mail, data centre (servers) and network services.

8.0 METHOD OF EXCHANGE OF INFORMATION

8.1 Personal information covered by this Agreement will be provided using protocols, formats, methods and technology agreed upon by both Parties to be defined in the Annexes to this Agreement so as to provide for secure, efficient, effective and timely disclosure of information from one Party to the other.

8.2 The Parties agree to review various modalities of transmission to ensure each Party's compliance with its respective legislation, policies and procedures relating to the transmission of personal information.

8.3 The Parties agree that it is not mandatory for the information to be disclosed through an automated system.

8.4 The Parties will, when transmitting information under this Agreement:

9.0 INFORMATION MANAGEMENT AND SECURITY REQUIREMENTS

9.1 In addition to Section 6, all personal information obtained under this Agreement will be collected, used, maintained, stored, retained, disclosed, destroyed or disposed of and otherwise administered and protected in accordance with all applicable legislation.

UNCLASSIFIED

9.2 The Parties will take all reasonable measures to observe their respective Information Management and Security requirements to ensure the confidentiality and integrity of information they receive under this Agreement and to safeguard that information against accidental or unauthorized access, disclosure, use, modification and deletion.

9.3 Each Party is responsible for keeping *Info Source* and all related Personal Information Banks up to date.

9.4 ESDC will follow any applicable legislation governing the protection of information including Part 4 of DESDA, the *Privacy Act*, the *Library and Archives of Canada Act* and regulations made under any of the foregoing and any other applicable federal legislation, the Government of Canada's Policy on Government Security, the Electronic Documents and Records Management Solutions Standard, and other related Policies, Standards and Directives, as well as all applicable departmental policies, protocols, operating directives, and guidelines, covering the administrative, technical and physical safeguarding, and disposal, of the personal information.

9.5 The CBSA will follow any applicable legislation governing the protection of information including the *Immigration and Refugee Protection Act*, the *Canada Border Services Agency Act*, the *Privacy Act*, the *Library and Archives of Canada Act* and regulations made under any of the foregoing and any other applicable federal legislation, the Government of Canada's Policy on Government Security, the Electronic Documents and Records Management Solutions Standard, and other related Policies, Standards and Directives, as well as all applicable departmental policies, protocols, operating directives, and guidelines, covering the administrative, technical and physical safeguarding, and disposal, of the personal information.

9.6 Where necessary and as agreed by the Parties, these obligations may be further specified in additional documents or agreements relating to the technology to be used.

9.7 ESDC and the CBSA will take such reasonable security measures to protect the confidentiality of the personal information exchanged under this Agreement. Security Measures are described in Annex F.

10.0 ACCURACY OF INFORMATION

10.1 Each Party will take all reasonable measures to maintain complete, accurate and up to date personal information for exchange under this Agreement. However, it is understood and agreed that they cannot guarantee its accuracy and completeness and will, therefore, not be held responsible by the other party for any damage resulting from the transmission or use of any information that is inaccurate or incomplete.

UNCLASSIFIED

10.2 The Parties will promptly notify the other if it learns that inaccurate information may have been disclosed and take all reasonable remedial steps to address the situation.

11.0 INVESTIGATION OF UNAUTHORIZED ACCESS, USE, DISCLOSURE, ETC

11.1 Provided that a disclosure or a failure to disclose personal information is done in good faith and reasonable care has been taken to comply with the applicable federal or provincial legislation, the Parties will not assume any liability whatsoever for the misuse of the personal information provided to the other under this Agreement. The security measures in effect with the Parties serve to maintain the integrity and confidentiality of the information disclosed to the other.

11.2 The Parties will each be responsible for the actions of their employees and agents with respect to the collection, disclosure, use, retention and disposal of personal information in their custody or under their control.

11.3 The Parties will investigate all cases where they have reasonable grounds to believe that any of the conditions set out in this Agreement has been or are likely to be breached by them, their employees or agents according to their internal protocols and procedures. This includes any case where it is alleged, suspected, or there is evidence that there has been unauthorized access, use, disclosure or modification of the personal information exchanged under this Agreement, modification of a permitted use, misuse or breach of confidentiality, or any incident which might jeopardize or has jeopardized the security or integrity of their respective computer systems or networks used to access and transmit the personal information, all or any of which are referred to as a Security Breach.

11.4 For ESDC, the procedures to be followed in an investigation are found in the Departmental Directive on How to Respond to Security Incidents Involving Personal Information, and any successor document. For CBSA, the procedures are found in the Security Volume- Physical Security Standards for Security Incident Reporting and in the Corporate Affairs Branch document entitled *Canada Border Services Agency Privacy Breach Protocol*.

11.5 In the event of a Security Breach, ESDC or the CBSA will immediately advise the other Party, and provide a detailed written report of the circumstances of any Security Breach and any remedial actions taken.

UNCLASSIFIED

11.6 Notice to ESDC will be sent to:
Director
Policy and Program Design Division
Temporary Foreign Worker Directorate
Employment and Social Development Canada
Place du Portage, Phase IV
140 Promenade du Portage
Gatineau, Québec
K1A 0J9

Director, Access to Information and Privacy
Employment and Social Development Canada
Place du Portage, Phase IV
140 Promenade du Portage
Gatineau, Québec
K1A 0J9

11.7 Notice to the CBSA will be sent to:
Director
Program and Policy Management Division
Traveller Programs Directorate
Canada Border Services Agency
191 Laurier Avenue West
Ottawa, Ontario
K1A 0L8

Director General
Security and Professional Standards
Canada Border Services Agency
410 Laurier Avenue West
Ottawa, Ontario
K1A 0L8

Director, Access to Information and Privacy Division
Canada Border Services Agency
410 Laurier Avenue West
Ottawa, Ontario
K1A 0L8

Director, Enforcement and Intelligence Policy Division
Canada Border Services Agency
100 Metcalfe Street
Ottawa, Ontario
K1A 0L8

UNCLASSIFIED

11.8 Upon being notified of a Security Breach, ESDC or the CBSA so notified may do any of the following on receipt of the notice:

- a) review the steps proposed by the other Party to address or prevent a recurrence of the Security Breach;
- b) direct that any additional specific steps be taken to prevent a recurrence;
- c) suspend the disclosure of personal information under this Agreement until satisfied that the other Party has complied with the Agreement and any directions; or,
- d) terminate this Agreement pursuant to section 17.

12.0 INFORMATION MANAGEMENT AUDIT

12.1 ESDC and the CBSA are both, and will remain, subject to their own internal audit procedures to ensure compliance with their program goals and statutory mandate, including compliance with this Agreement.

12.2 ESDC and the CBSA will provide a copy of their respective audit reports to each other, as applicable.

12.3 Where deficiencies in ESDC's or the CBSA's information management practices affecting compliance with the requirements of paragraphs 8 to 10 or the security, confidentiality and integrity of information exchanged under this Agreement are identified in an audit report, the body concerned will take appropriate corrective action forthwith to remedy those deficiencies.

12.4 With a view to improving services, privacy protection, and the efficiency and effectiveness of authorized information sharing, ESDC and CBSA will conduct routine information sharing sessions regarding program, business, and technology re-engineering plans, on a mutually agreeable schedule.

13.0 PRIVACY IMPACT ASSESSMENTS

13.1 The Parties will comply with the Treasury Board policies related to the completion of a Privacy Impact Assessment (PIA) and a Threat and Risk Assessment (TRA) covering the exchange of personal information under this Agreement. The Parties agree to provide a copy of the relevant portions of the related reports to each other.

13.2 Where issue(s) are identified in either the PIA or the TRA, the Parties agree to work together to address the issue(s).

13.3 When an issue cannot be resolved to the satisfaction of both Parties, it will be referred to Dispute Resolution as provided for in section 19 of this Agreement.

UNCLASSIFIED

14.0 COMING INTO FORCE

14.1 This Agreement will come into effect at the time it is last signed and will remain in effect until terminated by the Parties in accordance with Section 17 or replaced by another agreement.

14.2 This Agreement will be reviewed at least once every five years to ensure that it remains up to date and to make any amendments that may be required.

15.0 AMENDMENTS

15.1 Subject to paragraph 14.2, amendments to the terms of this Agreement will be made by an amendment executed by the Designated Representative (paragraph 18.1) of each Party in writing.

15.2 Amendments to the information to be disclosed as set out in the Annexes to this Agreement will be approved by the Designated Representatives (paragraph 18.1) of each Party. Any other amendments will be approved at the level of the Deputy Minister of the parties to this Agreement unless otherwise duly authorized by law.

16.0 FINANCIAL AGREEMENTS

16.1 Each Party will bear any costs they may incur in carrying out their obligations under this Agreement unless otherwise agreed to in writing.

17.0 TERMINATION

17.1 Either Party reserves the right to terminate this Agreement by giving 90 days written notice to the other Party.

17.2 In the event of the termination or amendment of this Agreement, the protection of information provisions set out as part of this Agreement continue to apply to and in respect of the information that has already been disclosed under this Agreement.

17.3 The Parties reserve the right to terminate this Agreement in the event of non-compliance with the terms of this Agreement. The Party wishing to terminate this Agreement will send to the other a written notice of termination stating the reasons for terminating; the latter Party will upon receipt of this notice, take measures to remedy the situation to the satisfaction of the first Party within thirty (30) business days of the notice or such further time period agreed upon by the Parties, failing which the Agreement will be automatically terminated.

UNCLASSIFIED

17.4 The following provisions survive the termination or expiry of this Agreement and continue in full force and effect, and do not merge: Section 6, Section 9 and Section 10.

18.0 MANAGEMENT AND GOVERNANCE

18.1 ESDC and the CBSA agree to each designate representatives to act as their contact persons for any issues related to the development, implementation, and administration of this Agreement.

For ESDC: Director General, Temporary Foreign Worker Directorate
 Employment and Social Development Canada

For the CBSA: Director General, Traveller Programs
 Canada Border Services Agency

Director General, Enforcement and Intelligence Programs
 Canada Border Services Agency

18.2 The Designated Representatives may appoint delegates to review the Agreement and provide advice on the development, implementation and administration of the Agreement and the adequacy of any privacy measures.

18.3 The delegates may meet as necessary to conduct these activities and to review any audit reports.

19.0 DISPUTE RESOLUTION

19.1 In the event of a dispute between the Parties arising out of this Agreement or Annexes, the Parties agree to make every effort to resolve it at the levels within their respective organizations at which the dispute arose. If any dispute remains unresolved by this process within fifteen business days of notification of the dispute, or such further period as may be agreed upon by the parties, the Parties agree that the dispute will be escalated to the Designated Representatives identified in Section 18 of this Agreement for resolution.

20.0 NOTICE

20.1 The Parties undertake to provide each other, as soon as practicable, notice of any change in legislation, regulation, policy, computer systems or funding relating to their respective programs that may impact either Party's ability to fulfill the obligations as described in this Agreement.

20.2 The Parties agree to advise and consult the other party at least six (6) months in advance, or as early as is otherwise possible, if information technology

UNCLASSIFIED

changes will affect the availability, means of access, or reliability of the information agreed to be exchanged.

20.3 Any notice or communication between the Parties, with the exception of the information exchanged for the purpose of Paragraphs 4, 5 and 7 of this Agreement that is required or permitted pursuant to this Agreement will be in writing by the Designated Representative.

21.0 GENERAL

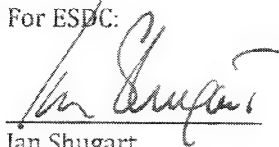
21.1 The Annexes to this Agreement are an integral part of this Agreement and are as follows:

- Annex A- Definitions
- Annex B- Record Disposition Authorities
- Annex C- Information to be provided by ESDC to the CBSA under section 34(1) and of the DESDA
- Annex D- Information to be provided by ESDC to the CBSA under section 35(1) of the DESDA
- Annex E- Information to be disclosed by the CBSA to ESDC
- Annex F- IT Security and IT Problem Management

21.2 This Agreement may be executed by the Parties in separate counterparts, each of which when so executed and delivered will be an original, and all such counterparts may be delivered by facsimile or electronic (email) transmission and such transmission will be considered an original.

IN WITNESS WHEREOF this Agreement has been signed on behalf of the Parties by their duly authorized representatives.

For ESDC:



Ian Shugart
Deputy Minister
Employment and Social Development
Canada

27.3.15.

Date

For the CBSA:



Luc Portelance
President
Canada Border Services Agency

2015-04-16

Date

UNCLASSIFIED

ANNEX A Definitions

"Access" – is the action from which an individual or organization collects, views, uses, discloses, manages and retains information described in the Agreement. This also includes connectivity to IT systems, paper forms or information in any other format.

"Authorized User" – employees who have been granted access to the personal information and aggregate data identified in this Agreement in accordance with the security requirements set out in this Agreement.

"Criminal Investigation Information Management System (CIIMS)" – CIIMS is the principal information management system used by employees in the CBSA's Criminal Investigations Program.

"Economic Class Permanent Residents (ECPR)" – refers to the economic class under which foreign nationals may apply and are selected for permanent residency to Canada. Applicants are selected on the basis of their ability to become economically established in Canada.

"Foreign Worker System (FWS)" – the FWS is ESDC's single, integrated system used internally to process applications for LMIA's and to track employer compliance with Program requirements. The FWS stores only the personal information required to process LMIA's and conduct assessments of employer compliance. The personal information collected includes, but is not limited to, client identification (i.e., family name and given names, gender, date of birth, country of birth, etc.), contact information and history, job offer information, compliance history etc.

The FWS provides a level of protection that reflects ESDC's need for information availability and integrity, Government of Canada requirements for protected B level information, and the requirements of the Privacy Act and associated Treasury Board policies. The FWS also responds to key data exchange agreements with other federal departments and acts as an efficient means of exchanging data on the outcomes of LMIA's and compliance assessments.

"Global Case Management System (GCMS)" – the GCMS is a single, integrated and worldwide system used internally to process applications for citizenship and immigration services. GCMS stores only the type of personal information required to process citizenship and immigration applications.

UNCLASSIFIED

"Field Operations Support System (FOSS)" - FOSS is an electronic system of record in which CIC and CBSA officers enter and obtain information about immigration and citizenship clients. The information obtained from FOSS is used to facilitate decisions in immigration, citizenship, and enforcement cases.

"Integrated Customs Enforcement System (ICES)" - ICES is a repository for CBSA enforcement-related information.

"Intelligence Management System (IMS)" - IMS and its Occurrence Reporting System (ORS) sub-module, is a CBSA system used to house intelligence information.

"Labour Market Impact Assessment (LMIA)" - is the opinion provided by ESDC or CIC in accordance with section 203 of the IRPR. In assessing requests for LMIA's, ESDC considers whether the employment of a foreign worker is likely to have a positive or neutral effect on the Canadian labour market. The LMIA is used to support the application of a foreign national for a work permit when required under IRPR.

"National Case Management System (NCMS)" - NCMS is the CBSA's primary immigration enforcement case management system.

"Personal Information" - Personal Information as defined in section 3 of the *Privacy Act*.

"Temporary Foreign Worker" - refers to any foreign national who has been authorized to work temporarily in Canada under the IRPA.

"Temporary Foreign Worker Program (TFWP)" - refers to the streams under which an employer who wished to hire a foreign worker must obtain an LMIA from ESDC.

"Secure Tracking System (STS)" - STS is a storage and information system used at the CBSA, which plays a role in screening immigration applicants.

UNCLASSIFIED

ANNEX B

Record Disposition Authorities

1.0 RECORD DISPOSITION AUTHORITIES

1.1 The TFWP has a Library and Archives Canada record disposal authority (RDA) document 2007/002 in place. Archival/historical and non-archival records are retained and then sent to LAC 2, 5, 7 or 10 years (depending on type of document) after completion or after becoming obsolete/superseded. Documents from regional and local ESDC offices are retained and then sent to LAC 5 or 10 years (depending on type of document) after completion or after becoming obsolete/superseded.

1.2 The CBSA has a Library and Archives Canada record disposition authority Immigration 2006/004 and 00/033. CBSA documents are subject to the following various retention periods: 2, 3, 5, 7, 10, 15 or 20 years. Documents are sent to private storage facilities (depending on the type of document and corresponding retention period) after becoming obsolete or superseded.

UNCLASSIFIED

ANNEX C

Information to be provided by ESDC to the CBSA under Section 34(1) of the DESDA:

1.0 METHOD OF INFORMATION EXCHANGE

1.1 For the issuance of a Work Permit

The data elements listed in section 2 may be disclosed to the CBSA for the assessment and issuance of a Work Permit.

1.1.1 Electronically, the CBSA has view only access in FOSS to the Foreign Worker System (FWS) – Global Case Management System (GCMS) system-to-system interface. Via this interface, the CBSA will have view only access to those data elements identified with an asterisk in the table below.

1.1.2 The FWS-GCMS interface gives the CBSA real-time access to information stored in ESDC's database. Personal information available via the FWS-GCMS interface may be linked to allow for automatic information exchanges and to enable the CBSA to view ESDC's FWS.

1.1.3 If not available via the system-to-system interface, this information can be made available electronically
 or paper copy of the original document(s).

1.1.4 A written request for information not available via FWS-GCMS interface will include, at a minimum, the following information: the requesting officer name, the requesting officer position, requesting officer contact information (telephone and/or email), description of personal information elements requested, legislative statute and associated section reference(s) and purpose (description of enforcement activity) for which the information will be used.

1.1.5 ESDC is responsible for the administration and maintenance of the
 The CBSA will have access to this in order to deposit and extract the agreed upon information.

1.1.6 The is designed to meet all the security requirements for exchanging personal information. The exchange of information will be protected from unauthorized access since both parties will be using
 capability to access and use the
 Approved user(s) will be given access codes to ESDC's to
 retrieve source files.

1.1.7 ESDC will upload data elements to the as per section 2 of Annex C on a case by case basis, as requested by the CBSA.

UNCLASSIFIED

1.1.8 A notification email will be sent to the designated approved user, confirming data transfer success.

1.1.9 If a paper copy of the information is requested, it will be provided directly to the requesting CBSA Officer as per Government Security Policy Guidelines.

2. DATA ELEMENTS TO BE DISCLOSED BY ESDC TO THE CBSA

2.1 Personal Information contained in the following table related to a LMIA may be made available to the CBSA:

Data Element(s) <i>(The CBSA will have view only access to those data elements identified with an asterisk in the table)</i>
Business Information
*Employer ID
*Employer CRA BN
*Employer business and legal name
*Employer mailing address, including street number, city, province, postal code, phone number and fax number.
*Employer business address (if different than mailing address), including street number, city, province, postal code
Type of Business
Response to Question: Is the business a franchise?
Response to Question: If the business is a franchise, is the corporate head office aware of this application for TFWs?
*Website address
*Date business started
*Describe the main business activity
*Principal contact name
*Telephone number + extension if applicable, fax number and e-mail address
*Contact Job Title
*Preferred Official Language of Correspondence
Third-Party, Recruiter or Employment Agency Information
Response to Question: Are you using the services of a third-party, recruiter or employment agency for the purposes of hiring a TFW?
Name of third-party, recruiter or employment agency for the purposes of hiring a TFW
Registration, license or certificate number
Response to Question: Are you appointing a third-party to represent you in completing this application form or to provide advice in and immigration process?
Name of third-party representative
Response to Question: Have you the employer or any other third-party in connection to this job offer received payment from the TFWs to secure this offer of employment?
Business Details
Number of employees currently employed nationally under this CRA Business number
Total number of employees currently employed at the work location specified on this form
Number of Canadians/permanent resident employees at work location covered by this LMIA
Total number of TFWs at the work location specified on this form
Response to Question: Did you employ a TFW in the last two years, prior to December 31, 2013?
Response to Question: Did you provide all TFWs employed by you in the last two years with

UNCLASSIFIED

Data Element(s) <i>(The CBSA will have view only access to those data elements identified with an asterisk in the table)</i>
wages, working conditions and employment in an occupation that were substantially the same as those that were described in the offer(s) of employment?
Response to Question: Have you applied for and received a positive LMIA on or after December 31, 2013?
Response to Question: Did you provide all TFWs employed by you, on all LMIAs received on or after December 31, 2013, with employment in the same occupation as described in the offer(s) of employment and with substantially the same wages, working conditions – but not less favourable than – those set out in that offer(s) of employment?
Response to Question: Have you had an LMIA revoked within the previous 2 years from the date you submitted the application? If yes, date and system file number
Response to Question: Were any employees laid off in the past 12 months? If yes, how many? Reason(s) for layoff(s) and occupations affected
Response to Question: Does your business receive support through any Government of Canada program? If yes, name of program
Job Offer Information
*Job title
Number of TFWs requested on this job offer
*Expected duration of employment
*Expected start date of employment, if any
*Location of job: Number and Street, city, province and postal code
*Main duties of the job
*Educational requirements of the job
*Experience/skills requirements of the job
*Language requirements
Wage in Canadian Dollars and number of work hours and overtime hours rate
Response to Question: Is the employment seasonal?
*Benefits
*Other benefits
*Response to Question: Are there provincial/territorial/federal certification, licensing or registration requirements of the job? If yes, name of the certifying/licensing/registering body
Confirmation that the position is part of a union. If yes, name of the Union.
Response to Question: Has the union been consulted about hiring a TFW? If yes, what is the position of the union?
Response to Question: Have you attempted to recruit Canadians / permanent residents for this job?
Response to Question: What are the potential benefits to the labour market for offering this job to a TFW?
Rationale for the job offer to TFWs
Response to Question: Do you plan to hire or train Canadians / permanent residents for the position for which you are requesting an opinion?
Summary of Results to Meet Minimum Recruitment and Advertising Requirements
Number of applications/resumes received from Canadians/permanent residents
Number of Canadians/permanent resident applicants interviewed
Number of Canadians/permanent residents offered the position
Number of Canadians/permanent residents hired
Number of job offers declined by Canadians/permanent resident applicants
Number of Canadians/permanent resident applicants who were not qualified for the job
Impacts on the Canadian Labour Market
Response to Question: Will the entry of these TFWs lead to job losses, now or in the foreseeable future, for Canadians/permanent residents as a result of layoffs, outsourcing, offshoring or other factors related to utilizing TFWs?

UNCLASSIFIED

Data Element(s) <i>(The CBSA will have view only access to those data elements identified with an asterisk in the table)</i>
Response to Question: Is the job offer related to an activity, contract or a subcontract that will facilitate outsourcing or offshoring?
Film and Entertainment Requests
Name of Production
Total number of people involved in the production
Type of Production
Copy of the contract between the employer and the foreign entertainer(except for film and TV requests)
Temporary Foreign Worker Information
Surname as shown on passport
Given name as shown on passport
Gender
*Date of birth
*Location of residence outside of Canada
*Citizenship(s)
Location of TFW if in Canada and immigration Status
Declaration of Employer
Declaration of proprietorship
Signature of employer and third party (if applicable)
Caregiver Program
*Employer #1 and Employer #2 Given and last names
*Employer #1 and Employer #2 Work and home telephone numbers
*Employer #1 and Employer #2 Address: number/street/PO Box#
*CP Alternate contact person (spouse, common-law partner, other relative if applicable)
*Given and last
*Telephone number
Caregiver Job Offer Information
*Expected duration of employment (months or years)
Rationale for the job offer to the caregiver and explanation of how it meets the employment needs of the applicant
Number of dependents (including those that do not live in the household)
Relationship of the employer to person who will receive care (i.e., child care, care of elderly person, care of person with disability)
*Location of where care will be provided and where foreign caregiver will reside (address, city, province/territory, postal code)
*Describe the main duties of the job
*Language requirements (Oral: English, French, other. Written: English, French, other)
Accommodations charges (does not apply in Quebec)
Meal charges
Private furnished accommodation with lock provided
Number of sick days per year and per week
*Name of foreign caregiver as shown on passport
*Gender
*Date of birth
Seasonal Agricultural Worker Program
Total # of Canadian agricultural worker employed:
<ul style="list-style-type: none"> This year Last year
Total # of foreign agricultural worker requested:
<ul style="list-style-type: none"> This year

UNCLASSIFIED

Data Element(s) <i>(The CBSA will have view only access to those data elements identified with an asterisk in the table)</i>
• Last year
If the requested number of workers is different from last year/season, please explain:
List crops/commodities, acreage, and method harvested
Housing type
Housing inspection
Check one: Direct arrival, direct replacement, double arrival, double transfer, replacement transfer, double arrival, transfer
Schedule A: Appointment of a Third-Party Representative
Business Name
CRA Business Number
Legal Name
Third-Party ID#
Mailing Address including street number, city, province, postal code, phone number and fax number.
Business Address including street number, city, province, postal code, phone number and fax number.
Main activity of the business
Principal contact name
Job Title
Telephone Number
Fax Number
Email Address
Preferred Language of Correspondence
Name of Employer Business
Response to Question: The representative is unpaid and:
Response to Question: The representative is, has been or will be paid and is a member of good standing
Schedule B: Impact on the Canadian Labour Market
Name of Business
Employer Contact Name
Telephone Number
Alternate Telephone Number
Title
E-mail Address
Fax number
Name of Employer Applying for the LMIA
System File Number
Response to Question: Will the entry of TFWs lead to job losses, now or in the foreseeable future, for Canadians and/or permanent residents as a result of lay-offs, outsourcing, offshoring or other factors related to the utilizing TFWs?
Response to Question: Does this contract or a subcontract facilitate outsourcing or offshoring?
Schedule C: Employer Transition Plan
Business Name
CRA Business Number
Legal Name
Business Operating Name
Business Address including street number, city, province, postal code
Occupations of positions requested
Number of positions requested on the LMIA application
Number of Canadian/permanent resident employees currently employed in the occupation at the

UNCLASSIFIED

Data Element(s) <i>(The CBSA will have view only access to those data elements identified with an asterisk in the table)</i>
work location
Number of foreign workers currently employed in the occupation at the work location
Total number of employees currently employed at the work location specified on the LMIA application
Number of employees currently employed nationally under this CRA business number
Seasonal occupation, if yes, peak employment season and total workforce during that time
Response to Question: Have you completed a Transition Plan for this occupation at this work location before? If yes, did the number of TFWs decrease relative to the number of Canadians/permanent resident workers for this occupation at this location as a result of activities conducted in the Transition Plan.
Description of planned activities
Proposed dates for activities
Results of planned activities
Actual results of activities
Milestones/benchmarks for activities, proposed and actual result <ul style="list-style-type: none"> • Total number of applicants • Total number of applicant interviewed • Total number of positions offered • Total number of applicants hired
For each activity, rationale for not hiring Canadians/permanent resident candidates
Employer Compliance
Employer Compliance Review (ECR) Results: Wages, Occupation and Working Conditions (WOW) of the LMIA confirmation <ul style="list-style-type: none"> • employer name and contact information • job title, occupation and NOC codes • results of findings, including areas of non-compliance and associated corrective actions to be undertaken • findings of non-compliance • ECR period
Inspection Results: Conditions of the LMIA confirmation <ul style="list-style-type: none"> • employer name and contact information • job title, occupation and NOC codes • results of findings, including areas of non-compliance and associated corrective actions to be undertaken • findings of non-compliance • inspection or review period
Ministerial Instructions: <ul style="list-style-type: none"> • employer name and contact information • job title, occupation and NOC codes • type of instruction ordered date of decision

UNCLASSIFIED

ANNEX D

Information to be provided by ESDC to the CBSA under section 35(1) of the DESDA:

1.0 METHOD OF INFORMATION EXCHANGE

1.1 The Data elements listed in Section 2 of Annex C and Section 2 of Annex D may be disclosed to the CBSA under section 35(1).

1.2 Disclosures under Annex C may be made on ESDC's own initiative or by written request from the CBSA.

1.2.1 Electronically, the CBSA has view only access in FOSS to the Foreign Worker System (FWS) – Global Case Management System (GCMS) system-to-system interface. Via this interface, the CBSA have view only access to those data elements listed in Section 2 of Annex C.

1.2.2 If not available via the system-to-system interface, this information can be made available electronically
 or paper copy of the original document(s).

1.2.3 A written request from the CBSA will include, at a minimum, the following information: the requesting officer name, the requesting officer position, requesting officer contact information (telephone and/or email), description of personal information elements requested, legislative statute and associated section reference(s) and purpose (description of enforcement activity) for which the information will be used.

1.2.4 If a paper copy of the information is requested, it will be provided as per Government Security Policy Guidelines.

1.2.5 ESDC is responsible for the administration and maintenance of the . The CBSA will have access to this site in order to deposit and extract the agreed upon information.

1.2.6 The s designed to meet all the security requirements for exchanging personal information. The exchange of information will be protected from unauthorized access since both parties will be using . capability to access and use the
 Approved user(s) will be given access codes to ESDC's to retrieve source files.

1.2.7 ESDC will upload data elements to the as per Section 2 of Annex C on a case by case by case basis, as requested by the CBSA.

UNCLASSIFIED

1.2.8 A notification email will be sent to the designated approved user, confirming data transfer success.

2. ADDITIONAL DATA ELEMENTS TO BE DISCLOSED BY ESDC TO THE CBSA

2.1 Personal Information, in addition to that collected on the LMIA Application form (listed in Annex C), related to the assessment of an LMIA may be made available to the CBSA upon request:

- the third party representative authorization form and contract between third party and employer
- proof of advertising
- business license
- T2 Schedule 125 Income Statement
- T2 Schedule 100 Balance Sheet
- Workers' Compensation Clearance Letter
- employer/employee contract
- correspondence between ESDC/Service Canada and employer or authorized third party
- labour market decision letter issued to the employer
- guarantor attestation for Caregiver stream
- Employer Compliance Review (ECR) Findings, including:
 - employer name and contact information
 - job title, occupation and NOC codes
 - results of findings, including areas of non-compliance and associated corrective actions to be undertaken
 - outcome of non-compliance
 - ECR period
- Inspection Findings, including:
 - employer name and contact information
 - job title, occupation and NOC codes
 - results of findings, including areas of non-compliance and associated corrective actions to be undertaken
 - outcome of non-compliance
 - inspection period
- Ministerial Instructions:
 - employer name and contact information
 - job title, occupation and NOC codes
 - type of instruction ordered
 - date of decision

2.2 Personal Information contained in the following documents related to the FSWP may be made available to the CBSA:

- the application form

UNCLASSIFIED

- the third party representative authorization form and contract between third party and employer
- the offer of permanent employment to the foreign national
- copies of remittance forms issued by the Canada Revenue Agency (CRA) itemizing source deductions for the previous 12 months (form number PD7A) as well as CRA T4 "Summary of remuneration paid" for the previous tax year
- CRA Notice of Assessment
- Signed T2 (corporate Income Tax Return) and T212
- T2125 Statement of Business or Professional Activities
- business licenses spanning 12 months or a commercial lease agreement for the business location
- correspondence between ESDC/Service Canada and employer or authorized third party related to the application

ESDC may, upon request or on its own initiative, and as appropriate, disclose information related to ESDC's responsibilities under the IRPA to the CBSA for the purpose of investigating any other alleged non-compliance with IRPA.

UNCLASSIFIED

ANNEX E

Information to be disclosed by the CBSA to ESDC:

1.0 METHOD OF INFORMATION EXCHANGE

1.1 For Employer Compliance Activities

The data elements listed in Section 2 of Annex E may be disclosed to ESDC for the assessment of employer compliance activities.

1.1.1 This information may be made available electronically or paper copy of the original document(s).

1.1.2 ESDC is responsible for the administration and maintenance
 The CBSA will have access in order to deposit the agreed upon information.

1.1.3 The is designed to meet all the security requirements for exchanging personal information. The exchange of information will be protected from unauthorized access since both parties will be using to access and use

1.1.4 A written request for information not available via FWS-GCMS interface will include, at a minimum, the following information: the requesting officer name, the requesting officer position, requesting officer contact information (telephone and/or email), description of personal information elements requested, legislative statute and associated section reference(s) and purpose (description of enforcement activity) for which the information will be used.

1.1.5 The information will be extracted from the FWS database and formatted for use

1.1.6 In order to match the (TFWP) employer information with information from CBSA, ESDC will use a matching process

1.1.7 If a paper copy of the information is requested, it will be provided as per Government Security Policy Guidelines.

2.0 DATA ELEMENTS TO BE DISCLOSED BY THE CBSA TO ESDC

2.1 Upon request, or on its own initiative, as appropriate, the CBSA will disclose the following information to ESDC for the purposes of assessing requests for LMIA's, reviewing such opinions or carrying out an inspection under the IRPR:

UNCLASSIFIED

- information related to anyone who has submitted an application under the TFWP/FSWP and for which charges have been laid as well as when convictions are rendered
- aggregate and non-case specific statistical information on TFWP-related criminal investigations
- additional information as may be requested by ESDC and for which the CBSA has the authority to disclose under the *Privacy Act*, but excluding the disclosure of case-specific information pertaining to ongoing criminal investigations
- convictions under IRPA of individuals or employers who requested or received an LMIA
- information received by the CBSA, including tips from third parties, that may not warrant criminal investigation and would instead be more appropriately addressed through regulatory actions by ESDC

2.2 The CBSA commits to informing ESDC prior to undertaking public communications activities related to a TFWP-related criminal investigation.

2.3 The following information related to criminal charges/convictions will be shared with ESDC:

Data Element(s)
Surname (of Subject)
Given name(s) (of Subject)
Country of Residence (of Subject)
Date of Birth (of Subject)
Address (of Subject)
Business Number (if applicable)
Business Name (if applicable)
Operating Name(s) (if applicable)
Case Number
Criminal Investigations Office
Date Charges Laid
Date Prosecution Concluded
Act/Section under which charges were laid
Prosecution Results
Sentence(s)

Other information that is collected under the authority of IRPA may also be shared (e.g. details of fraudulent information that was included in LMIA requests). Requests would be assessed on a case-by-case basis.

UNCLASSIFIED

ANNEX F

IT Security and IT Problem Management

1. INFORMATION MANAGEMENT

- 1.1 The information received by each Party under the Agreement will be protected as provided for under the laws of Canada and in accordance with the Agreement, Section 7.0 and Annex F. Personal information is to be safeguarded by a high level of protection to ensure the quality, integrity, privacy and security of the disclosure process.
- 1.2 On the request of the CBSA, ESDC will provide information describing its security measures. ESDC will take such reasonable security measures to protect the confidentiality of the personal information exchanged under this Agreement, as may be required by the CBSA.
- 1.3 On the request of ESDC, the CBSA will provide information describing its security measures. The CBSA will take such reasonable security measures to protect the confidentiality of the personal information exchanged under this Agreement, as may be required by ESDC.
- 1.4 For ESDC:
 - 1.4.1 The methods of protection include physical measures, for example, locked filing cabinets and restricted access to offices; Departmental measures such as appropriate employee security clearance levels and limiting access to a "need-to-know" basis; and technological measures such as the use of passwords and encryption. ESDC make their employees aware of the importance of maintaining the confidentiality of personal information.
- 1.5 For the CBSA:
 - 1.5.1 The methods of protection include physical measures, for example, locked filing cabinets and restricted access to offices; Departmental measures such as appropriate employee security clearance levels and limiting access to a "need-to-know" basis; and technological measures such as the use of passwords and encryption. Through awareness, the CBSA makes their employees aware of the importance of maintaining the confidentiality of personal information.

2. ESDC IT SYSTEMS, SECURITY REQUIREMENTS AND ACCESS

- 2.1 ESDCs systems, FWS are subject to the Treasury Board Secretariats Policy on Government Security, Departmental Security

UNCLASSIFIED

Policy and Procedures Manual and Departmental Information Technology Security Policy.

- 2.2 All system access activities by ESDC personnel are logged for audit purposes with built-in verification procedures for detecting and controlling any improper or inappropriate use of shared or exchanged personal information.

2.2.1 The FWS

- 2.2.1.1 The FWS is a secure single, integrated system designed to meet all the security requirements for storing personal information.

- 2.2.1.2 The specific hardware components of the FWS include a secure web portal and server.

This hardware is not specific to FWS System.

- 2.2.1.3 To access FWS proposed users must undergo a security screening process. Only authorized users who require the personal information in the course of their employment and duties will have access to the FWS.

- 2.2.1.4

UNCLASSIFIED

3 THE CBSA IT SYSTEMS, SECURITY REQUIREMENTS AND ACCESS

- 3.1** It is the policy of the CBSA to safeguard CBSA program information and to share and use this information only within established guidelines that adhere to Canadian law, CBSA policy, Canada's international treaty obligations, and the Agency's Code of Conduct, and in support of the effective delivery of CBSA programs.

UNCLASSIFIED

- 3.2 It is the policy of the CBSA to adhere to relevant Treasury Board Policy, including the *Policy on Government Security*.
- 3.3 Prior to accessing CBSA systems, all CBSA personnel are required to obtain the required security clearance.
- 3.4 Access to CBSA systems, and the level of access to information stored in those systems, is based on an employee's duties and the requirements of the position.
 - 3.4.1 CIIMS
 - 3.4.1.1 The source of all information entered into this database is clearly identified.
 - 3.4.1.2 The source identifier remains permanently attached to the relevant information and is included in all query results.
 - 3.4.1.3 Access to CIIMS is controlled via profile levels, and is granted only to those profiles that require access for investigative purposes.
 - 3.4.2 FOSS
 - 3.4.2.1 Employee level of access to information in this system is based on the requirements of their position.
 - 3.4.2.2 Any record that is created in FOSS using ESDC information will clearly identify ESDC as the source of the information and will include applicable caveats and restrictions on use of the information.
 - 3.4.3 GCMS
 - 3.4.3.1 Employee level of access to information in this system is based on the requirements of their position.
 - 3.4.3.2 Any record that is created in GCMS using ESDC information will clearly identify ESDC as the source of the information and will include applicable caveats and restrictions on use of the information.
 - 3.4.4 ICES
 - 3.4.4.1 ESDC information will be used to create a record in ICES in very limited circumstances.
 - 3.4.4.2 Any record that is created in ICES using ESDC information will clearly identify ESDC as the source of the information and will

UNCLASSIFIED

include applicable caveats and restrictions on use of the information.

- 3.4.4.3 The record will also refer the user back to the source of the information.
- 3.4.4.4 Records in this database are purpose-specific, and user access to those records is restricted according to the requirements of the employee's position.

3.4.5 IMS

- 3.4.5.1 Any records created in IMS will be associated with caveats specifying restrictions on use and disclosure.
- 3.4.5.2 IMS access is strictly limited to members of the CBSA Intelligence Portfolio only.
- 3.4.5.3 All potential disclosures are reviewed at the Manager level.
- 3.4.5.4 IMS includes a systemic audit function and capability.

3.4.6 NCMS

- 3.4.6.1 Employee level of access to information in this system is based on the requirements of their position.
- 3.4.6.2 Any record that is created in NCMS using ESDC information will clearly identify ESDC as the source of the information and will include applicable caveats and restrictions on use of the information.

3.4.7 STS

- 3.4.7.1 The source and date of all information and documents stored in this system are clearly identified.
- 3.4.7.2 Access to STS is limited and restricted to users with Secret clearance and those approved by CBSA Intelligence, and subject to audit.
- 3.4.7.3 All proposed disclosures of information contained in this database are reviewed by CBSA Intelligence management.

4 IT PROBLEM MANAGEMENT

- 4.1 The Parties agree to resolve any IT problem management issues within their respective organizations where the problem arose.
- 4.2 The Parties agree that any irregular and/or suspicious activity that is detected by either Information Technology or Business Line staff will be reported and acted upon in accordance with each Party's respective operational guidelines.

UNCLASSIFIED

- 4.3 Where an IT problem is identified, each Party agrees to notify the other as soon as possible.